

CDCO Response to

# 25 Point Implementation Plan to Reform Federal Information Technology Management

“Cloud First” Action Plan

1.	Introduction.....	1
1.1.	Overview and Action .....	1
1.2.	About CDCO.....	2
2.	CDCO Vision for federal cloud computing.....	3
2.1.	What is Cloud Computing? .....	3
2.2.	Hosting Options.....	4
2.3.	Unmanaged Guest Cost Comparison (monthly) .....	5
2.4.	Scaling the Cloud .....	6
2.5.	Can any IT project be deployed to the Cloud?.....	6
3.	Elements of the CDCO-Hosted Private Cloud.....	7
3.1.	Logical Description .....	7
3.2.	Cloud Schematic/High-Level Diagram .....	8
3.3.	Fundamental Elements .....	9
3.3.1.	Virtualization and Cloud Service Delivery.....	9
3.3.2.	Processor and Memory .....	10
3.3.3.	Storage .....	10
3.3.4.	Backup .....	11
3.3.5.	COOP/DR and Data Replication .....	11
3.3.6.	Hardware and Software Monitoring .....	12
3.3.7.	National Service Desk (ITIL 3.0) .....	12
3.3.8.	Cloud Computing Operations Center (CloudOps).....	13
3.3.9.	Service Level Management.....	13
3.3.10.	Data Center Operations supporting the Cloud Infrastructure.....	13
4.	Summary.....	14

# 1. Introduction

## 1.1. Overview and Action

OMB<sup>1</sup> has directed the Federal Government be better prepared in the future. Agencies are now required agencies to deploy technology projects to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists. Agencies must reduce the need for infrastructure growth by implementing a “Cloud First” policy for services and increase their use of available cloud and shared services. OMB’s three-part strategy on cloud technology will revolve around using commercial cloud technologies where feasible, launching private government clouds, and utilizing regional clouds with state and local governments where appropriate.

To facilitate this shift, Department of Veterans Affairs (VA) Corporate Data Center Operations (CDCO) is establishing a secure government-wide private cloud computing platform based on the Infrastructure as a Service (IAAS) model.

CDCO plans on delivering cloud services via the *Infrastructure as a Service (IAAS)* service model in a private cloud deployment model.

IAAS provides the ability for the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

The CDCO cloud leverages many technology components and practices already in existence to deliver functionality in shorter timeframes and support the efforts of VA IT projects to deploy working business functionality in less than 6 months.

CDCO will also leverage multiple-award indefinite-delivery, indefinite-quantity (IDIQ) contracts call for in the 1994 Federal Acquisition Streaming Act (FASA) to support the rapid delivery of cloud functionality.

The key to the success of the CDCO cloud offering is virtualization. Using virtualization, operating system images are dissociated from physical platform and run as one or more “guests” on redundant hardware.

The CDCO cloud infrastructure will be operated as a *VA private cloud*.

The cloud infrastructure is shared by VA organizations and supports the shared concerns of the VA community (e.g., mission, security requirements, policy, and compliance considerations).

---

<sup>1</sup> “25 Point Implementation Plan to Reform Federal Information Technology Management,” Office of Management and Budget, December 2010; <http://cio.gov/documents/25-Point-Implementation-Plan-to-Reform-Federal%20IT.pdf>

## 1.2. About CDCO

CDCO is a franchise fund, fee-for-service provider of Information Technology services for federal agencies, aligned under the VA Office of Information and Technology. CDCO operates five national data centers:

- Austin Information Technology Center (AITC)
- Hines Information Technology Center (HITC)
- Philadelphia Information Technology Center (PITC)
- Quantico Information Data Center (QITC)
- Capital Region Data Center (CRDC)

These centers are responsible for nearly \$100 billion in veterans' benefits, payments, and payroll processing for the Department as well as national health and benefits systems. The CDCO also operates the VA's Records Center and Vault, a storage facility for VA and other Federal agencies' records.



Figure 1 - CDCO Locations

In 1996, under Public Law (PL) 103-356, Government Management Reform Act (GMRA) of 1994, CDCO was approved as a franchise fund organization with the authority to offer IT products and services to other Federal agencies on a full cost recovery fee-for-service basis. Permanent status was conferred upon Department of Veterans Affairs (VA) Franchise Fund by PL 109-114 in FY 2006.

CDCO reports to the VA Franchise Fund Board of Directors, comprised of representatives from the various VA administrations and staff offices. The Board has management and oversight responsibility for the VA Enterprise Centers' rates, capital investments, budgets, and various franchise fund activities.

Since entering entrepreneurial government, CDCO has grown significantly by expanding services to our existing customers and by attracting new customers. In addition to VA customers, a sampling of other Federal agency customers includes Government Accountability Office (GAO), Department of Justice (DOJ), National Aeronautics and Space Administration (NASA), National Archives and Records Administration (NARA), General Services Administration (GSA), and many others.

Efforts to integrate common functions include the CDCO National Service Desk and CDCO Systems Security. Both are managed by AITC, but include staff from all Centers. By the end of FY 2009, CDCO Business Service will be similarly aligned.

CDCO service offerings are summarized in Table 1 below.

Cloud Computing	Infrastructure-As-A-Service (IAAS), virtual desktop integration (VDI)
Managed Hosting Services	CDCO hosts and manages over 2000 servers for multiple government agencies. Staffed service areas include system administration and programming (Microsoft Windows, Unix, IBM System Z), network administration, database administration (Oracle, SQL server, MySQL), Virtualization (IBM, VMware, Solaris), tiered and virtualized data storage/SAN, tape backups and security and 24 x 7 availability and performance monitoring.
Security Services/Information Assurance	Data protection with encryption, firewalls intrusion detection, vulnerability scanning and access control. Certification and Accreditation (C & A) of systems, data encryption, Expert support for adherence to FISMA, NIST, Privacy Act, OMB and VA and Federal guidance.
Enterprise Earned-Value and Business Office/Chargeback	Complete fee-for-service operation with chargeback based on actual costs in accordance with franchise requirements.
Business Continuity and Recovery	Continuation of operations planning using data replication, disaster recovery planning and testing.
Application Management	CDCO administers over 200 complex IT applications that support medical care, financial payments, benefits, record-keeping, and research programs.
Service Management	ITIL-based Change Management, Configuration Management, Incident Management and Problem Management processes in place.
Service Planning and Architecture	Requirements gathering, solution design, and implementation of physical and virtual solutions.

**Table 1 - CDCO Service Offerings**

## 2. CDCO Vision for federal cloud computing

### 2.1. What is Cloud Computing?

Cloud computing is a model<sup>2</sup> for enabling highly-available, convenient, on-demand access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with

<sup>2</sup> “NIST definition of Cloud Computing”, National Institute of Standards and Technology, October 2009; <http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc>

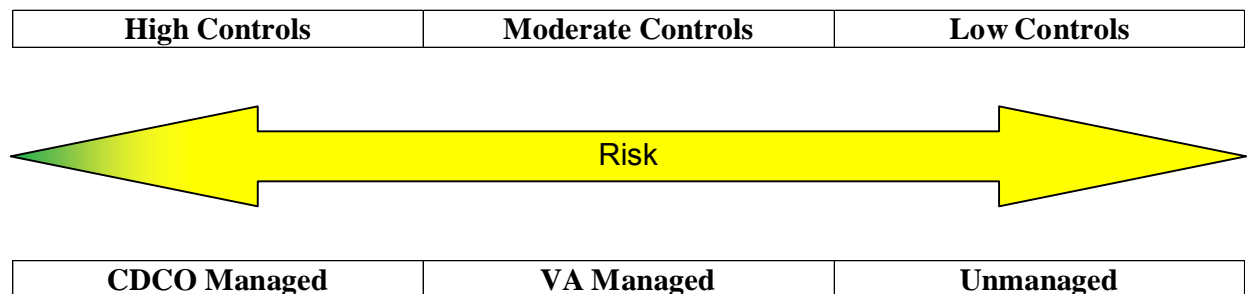
minimal management effort or service provider interaction. Cloud computing has five essential characteristics (see Table 2 below).

On-demand self-service.	A consumer can unilaterally provision computing capabilities automatically without requiring human interaction with each service's provider.
Broad network access	Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.
Resource pooling.	The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The customer generally has no control or knowledge over the exact location of the provided resources.
Rapid elasticity.	Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and in.
Measured Service	Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

**Table 2 - Essential Cloud characteristics**

## 2.2. Hosting Options

CDCO has identified a multi-faceted approach to cloud delivery that takes into account VA requirements. This approach should be suitable for almost all of the VA's IT deployment requirements. A key decision point is assessing impact levels for confidentiality, integrity, and availability as described in FIPS 800-60.



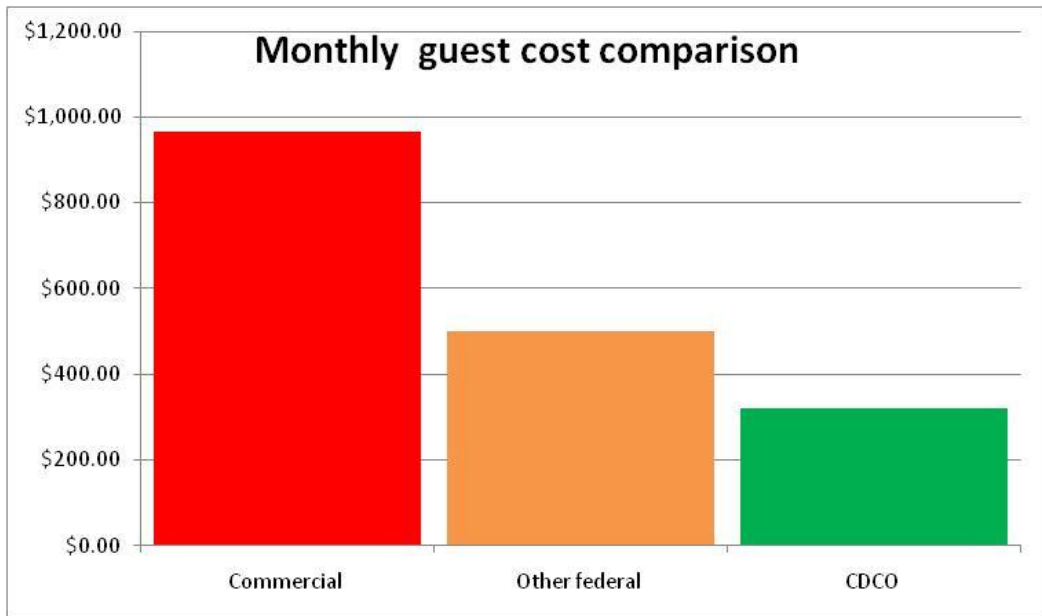
CDCO cloud environments are offered in accordance with the following template.

CDCO-Managed (Medium/High Impact) Production/PreProduction	VA Managed (Medium/High Impact) Production/PreProduction	Unmanaged (Low Impact) NonProduction	Internet-Facing
Guests in the cloud environment managed by CDCO IT Specialists (2210) and contract support according to strict ITIL service delivery criteria.	Guests in the cloud environment managed by VA IT Specialists (2210) and contract support.	Guests in the cloud environment managed by VA employees and contract support.	Virtualized guests (non-cloud) managed by CDCO IT Specialists (2210) and contract support according to strict ITIL service delivery criteria.

**Table 3 - Cloud Hosting Options**

2.3. Unmanaged Guest Cost Comparison (monthly)

Based on published FY2011 chargeback rates, CDCO conducted a cost comparison of virtualized platforms with a commercial provider used by the VA and another government cloud provider. Figure 2 shows that CDCO rates for similar cloud platforms are significantly less than what is available in the commercial and government market.



**Figure 2 - Cloud Cost Comparison**

## 2.4. Scaling the Cloud

One of the documented benefits of cloud deployment is scalability. CDCO will implement three aspects of cloud scalability

In the Federal CIO's 25 point implementation plan, the following example is used:

*“...The cloud allowed for a rapid response when demand jumped from 25,000 users to more than 250,000 users in three days, eventually reaching a peak rate of 20,000 new customers every hour. Because of the cloud, the company was able to scale from 50 to 4,000 virtual machines in three days to support increased demand on a real-time basis.”*

The first aspect of cloud scalability is inherent in virtualization technology. Specifically, service providers can add more guests to the same physical platform. As this happens, the guests consume more unused capacity until the physical platforms are saturated. This is a good short-term solution, but more is needed.

The second aspect of scalability is being able to rapidly expand the physical platform to extend the ability to create additional guests. CDCO will do this by executing a modular, repeatable infrastructure design, supported by an IDIQ contract that will allow specific components to be expanded based on requirements. This strategy is often referred to as a scale unit, virtualization block or vBlock in private industry.

The third aspect of scalability is leveraging other cloud providers for appropriate offloading of guests with low security impact. CDCO will also support this with an IDIQ contract with commercial cloud providers.

Despite cloud computing scalability potential, there are some software packages that do not support scalability. Federal acquisitions and development efforts should explicitly state the requirements for cloud computing platform support and priority for redeveloping and regression testing applications to ensure support.

## 2.5. Can any IT project be deployed to the Cloud?

Before deploying an application to the cloud, CDCO will conduct a “Cloud First” analysis to determine if this workload is appropriate for cloud deployment. There will be some workloads which are not appropriate for the cloud, based on system resource usage or program management. For example, a legacy application being replaced with an updated design in the next 12 months is probably not a good cloud candidate.

Workload requirements not suited:	<ul style="list-style-type: none"><li>• Exceeds 200 MB/second storage throughput</li><li>• Exceeds 5000 I/O operations per second</li><li>• Data store exceeds 1 TB</li><li>• Memory requirements exceed 128 GB</li><li>• Exceeds 100 MB/second network throughput</li><li>• DB/Exchange/Blackberry/HTTPS over 500 concurrent users</li><li>• Poorly designed or implemented software.</li></ul>
-----------------------------------	--

	<ul style="list-style-type: none"> <li>• Poor data management practices (retention/archive/logging).</li> </ul>
VA Requirement:	<ul style="list-style-type: none"> <li>• VA selected technology does not support cloud deployment.</li> <li>• Excessive cost for regression testing of application.</li> <li>• Program decision based on unspecified criteria.</li> </ul>

Table 4 - "Cloud First" considerations

### 3. Elements of the CDCO-Hosted Private Cloud

#### 3.1. Logical Description

The CDCO cloud builds on the virtualization infrastructure constructed over several years. The bottom level of the cloud is industry standard hardware provisioned in accordance with the VA Technical Reference Model and engineering standards. Above this is the cloud OS, most commonly VMware vSphere, but also including Oracle Solaris and IBM zLinux mainframe virtualization. This infrastructure allows the creation of "guest" virtual machines (VM) that represent what has been traditionally deployed as a physical server. Using a hypervisor, VMs can be created and used securely. The ability a VM to access private functions of the hardware is controlled by the hypervisor. In this way, the hypervisor limits the ability of a particular guest to affect another, a fundamental method of enforcing security.

Layered on top of this familiar infrastructure is the infrastructure authority; the interface that enables on-demand self-service. A consumer can unilaterally provision computing capabilities automatically without requiring human interaction with the service provider. The service provider establishes a virtual data center (VDC) for the consumer based on a contracted amount of processor, memory and storage. The consumer is then provided a secure, external interface to adjust and deploy those resources as requirements evolve.

In many cases, the consumer may not have the skilled staff required to manage their own services, or may desire to leverage advanced CDCO offerings, such as automated monitoring and scaling, 24 x 7 guest support or advanced security services. CDCO will leverage existing service offerings to provide these services.

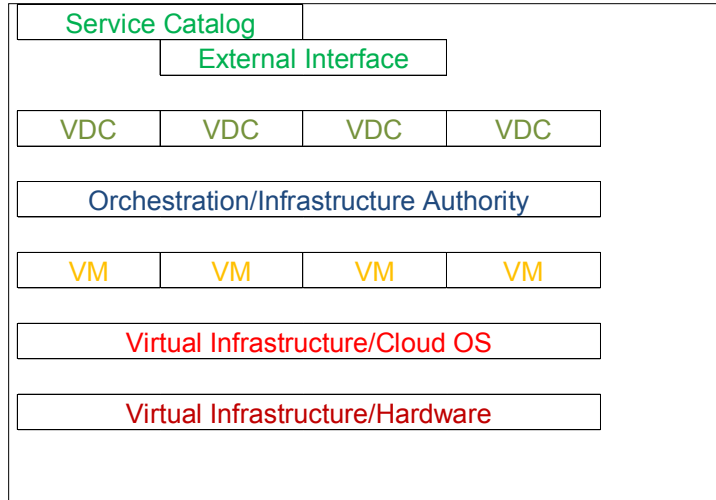


Figure 3 - Logical Cloud Design

### 3.2. Cloud Schematic/High-Level Diagram

As a VA facility, CDCO is able to leverage the existing network security and infrastructure in place. This infrastructure includes redundant telecommunications security screening and facilities that meet Uptime Institute standards. Within this infrastructure, data is protected with its own isolated, firewalled boundary.

Figure 4 shows the design schematic, with the failover datacenter. Consistent with the NIST cloud definition, there is a sense of location independence, in that the customer generally has no control or knowledge over the exact location of the provided resources. This diagram represents any pair of CDCO datacenters, not a specific location.

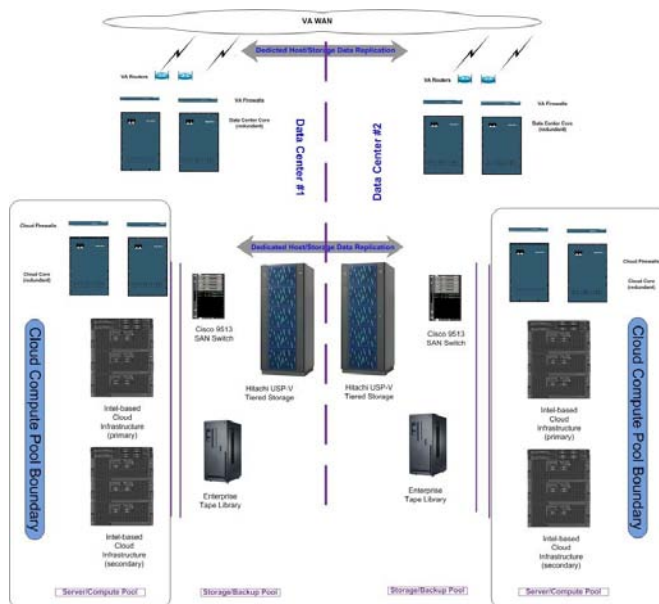


Figure 4 - CDCO High-Level Cloud Schematic

### 3.3. Fundamental Elements

**NOTE: Some of the services described in this section are available only with CDCO-managed cloud hosting.**

#### 3.3.1. Virtualization and Cloud Service Delivery

Selecting the virtualization environment (referred to as the Cloud OS) impacts subsequent design activities affecting the storage solution, server architecture, and network design. CDCO supports leading virtualization platforms including VMware's vSphere, Oracle Solaris containers and IBM zLinux. Although each product has its advantages, CDCO's primary solution for virtualization of Windows and Linux is VMware vSphere. VMware vSphere product is the market leader in the virtualization space, provides a robust virtualization platform, and provides advanced enterprise-level capabilities needed to support requirements. Regardless of the platform selected, the Cloud OS will support the following advanced features/capabilities:

- High Availability (HA) - Allows a failed guest to be restarted automatically.
- Dynamic Resource Scheduler (DRS) - Permits the pooling of memory and CPU resources to efficiently allocate resources to meet computing needs.
- Advanced Power Management (APM) - Monitors host servers and migrates guests and power down unneeded resources. APM will also be configured to provide additional processing capacity as required.

A key element of cloud services delivery is the infrastructure authority. VMware vCloud Director has been integrated with CDCO virtualization. Director delivers resources as virtual datacenters. Director logically pools compute, storage and networking capacity into virtual datacenters. CDCO is able to pool underlying infrastructure into tiers and offer these to users at discrete service levels and prices, rather than providing siloed physical infrastructures.

The infrastructure authority (IA) is the future nerve center of cloud infrastructure as a service (IaaS) operations. The IA provides a central metadata store, leverages common data models to request or offer services, maintains physical, virtual, and policy dependency maps, ensures security and regulatory compliance and integrates with third party management and orchestration tools to authorize IT operations such as provisioning or relocation before they proceed.

One of the 3<sup>rd</sup> party management tools CDCO uses is Veeam management suite, including backup, documentation/reporting, monitoring and business view.

Veeam is the #1 Backup for VMware environments with file-level restore for Windows and Linux, and built-in de-duplication. Veeam Reporter is the first reporting and change management solution specifically designed for large VMware environment and creates management reports and detailed documentation. Veeam Monitor enables performance monitoring, capacity planning and troubleshooting for VMware. Veeam Business View offers an automated, flexible and dynamic way to group guests within different categories: business unit, department, purpose and other. CDCO can see and manage the virtual infrastructure based on business needs and priorities with flexibility to define custom chargeback models.

### 3.3.2. Processor and Memory

Provisioning processor and memory for the cloud infrastructure leverages years of CDCO server architecture and design experience. The selected platform takes into consideration capacity planning, storage management, backup, disaster recovery, and network redundancy as well as the VA TRM. CDCO has selected and acquired Dell R810 rack-mount servers with dual Intel CPUs and 512 GB memory. Based on the virtualization of hundreds of VA workloads, CDCO has found guests typically consume more memory than CPU. While the systems have internal storage for page files and other purposes, all guest data will be stored on fibre channel storage subsystems.

### 3.3.3. Storage

CDCO uses industry best practice to selecting and configuring disks and disk groups to meet server performance and storage capacity requirements. The current target platform at CDCO sites is virtualized through a Hitachi USP-V. This allows data to be transparently migrated between storage performance tiers and various vendor storage subsystems without interrupting host operations. CDCO currently defines four storage tiers:

- Tier 1 – RAID 1+0 SCSI
- Tier 2 – RAID 6 SCSI
- Tier 3 – RAID 1+0 SATA
- Tier 3 – RAID 6 SATA

Redundant Array of Individual Disks (RAID) will be configured to support migrated applications, databases, and files stores. RAID configuration has an impact on overall system performance; CDCO will balance the performance impact with data protection requirements. At a minimum, RAID Level 6 (disk striping with dual parity) will be configured to protect enterprise data. RAID level 10 (mirrored disk striping with parity) will be considered for critical in data stores.

CDCO recognizes that beyond the physical design of the SAN, performance is influenced by load placement of the cloud data stores. Data stores layout, tiering

and placement will comply with best practices. For VMware, data store sizes will typically range between 500GB and 1TB which will be our target Logical Unit Number (LUN)/data store size. Individual data stores will be created for cloud server footprints larger than 1TB.

Storage is thin provisioned to support scalability and expansion and reduce cost. Thin provisioning is a method for optimizing utilization of available storage. It delivers on-demand allocation of blocks of data versus the traditional method of allocating all the blocks up front.

#### 3.3.4. Backup

CDCO has a mature tape backup infrastructure and process in place that supports data backup, encryption of tapes in accordance with VA 6500 and litigation holds for legal retention of data. CDCO has implemented an isolated network for tape backup to avoid conflict with normal data processing.

#### 3.3.5. COOP/DR and Data Replication

CDCO storage backup and disaster recovery design will be based on RPO/RTO requirements provisioned for existing CDCO customers. There are several approaches available to design for backup and recovery. COOP will be monitored and tested at regular intervals in order to ensure functionality. COOP/DR by its definition focuses on the broader business requirements of disaster planning. It addresses technical as well as business requirements. CDCO creates COOP/DR plans to include additional business requirements such as succession planning, and facilities management.

Our primary backup and recovery solution will be designed using SAN-based snapshots. SAN-based snapshots function at the SAN controller level at extremely high speeds which has the added benefit of offloading overhead from the server infrastructure. A SAN based system backup relies on a single full copy with sequential incremental snapshots performed at the block level. Integration of this technology is in almost all cases vendor and/or hardware specific. Our design analysis will assess the reuse of existing storage systems from the locations being decommissioned.

CDCO will also use technologies such as VMware Site Recovery Manager SRM). SRM provides disaster recovery failover capability between sites, and integrates with array-based replication hardware. As part of this approach, VMWARE vCenter management servers located at primary and recovery sites monitor system availability so that, if a guest at one site shuts down, the corresponding guest at the failover site starts up. Using the data replicated from the protected site, the recovery site will assume responsibility for providing the same services.

Migration of protected inventory and services from site to site will be controlled by a recovery plan. This plan specifies the order in which virtual machines are

shut down and started up, the resource pools that are allocated to each, and the networks they can access. SRM enables the ability to test a recovery plan, using a temporary copy of the replicated data, in a manner that does not disrupt ongoing operations at either site. The design approach takes into consideration that the replication performance is highly dependent on the network design, latency, and link capacity.

#### 3.3.6. Hardware and Software Monitoring

CDCO deploys basic monitoring by default in the cloud infrastructure. Basic monitoring tracks availability of hardware infrastructure primarily of physical servers and network. This is accomplished using approved VA toolsets such as BMC Patrol and Orion SolarWinds and Network Performance Monitor. Typically, there is no knowledge or integration of middleware or application with basic monitoring.

CDCO offers predictive and responsive monitoring for critical systems. This monitoring allows for diagnosis and proactive avoidance of issues and integrates fully with CDCO ITIL processes. Monitoring responds to thresholds based on intelligent modeling of internal and external system dependencies. This includes CMDB-aware, automated incident creation and tailored data feeds to reduce Mean Time to Repair (MTTR) metrics. Critical systems monitoring requires extensive analysis of applications and their dependencies based on interaction with development teams. Critical monitoring leverages a CA Technologies toolset including Spectrum Service Assurance, NetQOS and Application Performance Manager.

#### 3.3.7. National Service Desk (ITIL 3.0)

CDCO will leverage the CDCO National Service Desk infrastructure to operate and maintain the VA cloud. CDCO considers the Service Desk as not “just the help desk,” but rather a central point of contact for all IT service management functions.

The CDCO Service Desk is the core of support and the end users’ front line. CDCO has tailored SOPs to log incidents and service requests, provide first-line investigation and diagnosis, escalate incidents and service requests as needed, and communicate and keep all stakeholders informed on progress.

CDCO will perform activities to accurately and expeditiously resolve all technical problems connected with, but not limited to servers, network infrastructure, virtualization environment, data storage, and facilities.

All hardware, network connectivity, server, and networking failures/problems will be promptly reported to the appropriate personnel for rectification.

The service desk operates based on the Information Technology Infrastructure Library (ITIL) framework. ITIL is the most widely accepted set of integrated processes to support data center management and improve service delivery. CDCO has numerous personnel certified in ITIL to implement, manage, and improve processes to deliver high quality IT services.

CDCO ensures infrastructure changes follow strict configuration control and change management procedures.

### 3.3.8. Cloud Computing Operations Center (CloudOps)

CDCO will operate a cloud computing operations center as the primary work space to monitor, manage and troubleshoot problems within the cloud. CloudOps will be staffed with engineers and technicians to provide support twenty-four hours a day, seven days a week. This will provide the structure to effectively coordinate O&M activities with all participants, vendors, customers, and end-users of the datacenter.

CloudOps will offer oversight of problems, configuration and change management, network security, and performance and policy monitoring. CloudOps operational Standard Operating Procedures (SOPs) will interface/coordinate with CDCO National Service Desk, to respond to incidents and/or escalate problems.

### 3.3.9. Service Level Management

CDCO will collect real-time performance/quality information to ensure that performance targets (e.g. Service Level Agreements [SLAs]) are met.

The cloud environment will be continuously evaluated to ensure services meet business requirements and SLA metrics. CDCO will track metrics provide monthly trend analysis reports will identify recurring incidents and problem management, customer training needs, and process improvement opportunities.

### 3.3.10. Data Center Operations supporting the Cloud Infrastructure

Cloud Computing will leverage CDCO's qualified staff to execute processes and procedures for key operations necessary to maintain a healthy and responsive data center infrastructure to include:

- Systems Administration – CDCO system administrators will work on the cloud infrastructure and also on guest virtual platforms to provide the highest level of support. They will resolve tickets escalated from the service desk. System Administrators are considered subject matter experts and participate in the change control and quality improvement processes.

- Network Administration - CDCO network administrators monitor and secure the network for the cloud infrastructure. In addition, network administrators coordinate LAN and WAN connectivity requirements. Network Administrators are subject matter experts and participate in the change control and quality improvement processes. Network personnel monitor operations of backbone links and network devices, ensure continuous operation of network services, troubleshoot all network related problems and open tickets to track and document resolution of problems.
- Database Administration – CDCO database administrators (DBA) support Oracle and Microsoft SQL databases on guest virtual platforms to provide the highest level of support. They will resolve tickets escalated from the service desk. DBAs are subject matter experts and participate in the change control and quality improvement processes.
- Application Support - CDCO will monitor application performance proactively through the use of automated tools to ensure compliance with SLAs. CDCO application support provides special expertise in J2EE platforms, enterprise messaging and monitoring. Application support includes collaboration with application owners to troubleshoot, isolate, and rectify problems with their applications. In addition, this support will continually assess performance trends, anticipate areas of improvement, and leverage expertise to identify effective solutions for issues.
- Hardware/Software Support and Configuration/Asset Management - CDCO maintains comprehensive data regarding datacenter equipment to include warranty information, firmware, location, bar codes, etc via an ITIL Configuration Management DataBase (CMDB). CDCO understands the criticality of maintaining vendor support for all enterprise assets. The CMDB tracks and provide advanced notice to ensure renewal of vendor hardware maintenance contracts. CDCO will leverage the CMDB software license and maintenance renewals.
- Facilities - CDCO will ensure that facilities are maintained and will configure environmental controls by deploying and operating fire, power, temperature, and humidity monitoring systems. CDCO also ensures the physical security of the enterprise data center by implementing automated safeguards, commonly referred to as “guns, gates and guards.”

#### 4. Summary

OMB has directed federal agencies to implement a “Cloud First” policy for services and increase their use of available cloud and shared services. CDCO is establishing a secure government-wide private cloud computing platform based on the Infrastructure as a Service

(IAAS) model. CDCO is committed to providing quality cloud services through a highly reliable, robust, available, and secure computing environment.

CDCO offers a complete package of services, including IT operations, cost and accounting flexibility and a highly trained and motivated IT support staff. As a business partner with our customers, we are committed to keeping our focus on customer service and providing solutions that meet our customers' needs at competitive prices in order to maximize their investments in technology.

CDCO contracts with Gartner annually to conduct an independent satisfaction survey of customers. Of the nearly 300 surveys conducted within the peer group of both private sector and public sector organizations, CDCO scored within the top 12 percent of overall satisfaction scores.