

UNCLASSIFIED

DoD Information Enterprise Architecture



Core Data Center Reference Architecture

Version 1.0

Final

(Public Release Version)

September 18, 2012

Prepared by:

Director, Architecture & Interoperability
Office of the DoD Chief Information Officer

UNCLASSIFIED

UNCLASSIFIED

[This page intentionally left blank

UNCLASSIFIED

Table of Contents

Forward	1
Executive Summary	2
1.0 Strategic Purpose.....	3
1.1 Introduction & Overview	3
1.1.1 Purpose	3
1.1.2 What Is a Core Data Center?	3
1.1.3 Derivation of Content	4
1.2 Scope, Assumptions, Constraints and Intended Audience	4
1.2.1 Scope	4
1.2.2 Assumptions & Constraints	4
1.2.3 Intended Audience and Uses	5
1.3 Alignment with the Joint Information Environment.....	5
1.4 Architecture Development.....	6
2.0 The Vision for Computing Transformation in the Department	7
2.1 Overview and Problem Statement	7
2.2 Transformational Vision and High Level Goals.....	7
2.3 Support for Legal and Regulatory Mandates	8
2.3.1 Federal Data Center Consolidation Initiative (FDCCI).....	8
2.3.2 FY12 National Defense Authorization Act (NDAA)	9
2.4 The JIE Computing Infrastructure	9
2.5 Functional Perspective.....	11
3.0 Core Data Center Requirements	14
3.1 Facility Infrastructure.....	14
3.1.1 Overview	14
3.1.2 Principles and Rules	16
3.2 Computing Infrastructure.....	19
3.2.1 Overview	19
3.2.2 Principles and Rules	19
3.3 Capability Delivery	21
3.3.1 Overview	21
3.3.2 Principles and Rules	23

UNCLASSIFIED

3.4 Security and Information Assurance (IA) 24

 3.4.1 Overview 24

 3.4.2 Principles and Rules 28

3.5 Standardized Operations & Processes 31

 3.5.1 Overview 31

 3.5.2 Principles and Rules 33

Appendix A: Overview/Summary (AV-1) 40

Appendix B: Standards Viewpoint (StdV-1) 44

Appendix C: Operational Activity Node Tree (OV-5a) 51

Appendix D: Glossary and Integrated Dictionary 54

 D.1 - Glossary 54

 D.2 – Integrated Dictionary (AV-2) 57

Figures and Tables

Figure 1 - DoD Enterprise Perspective (OV-1_1) 10

Figure 2 - Notional CDC Floor Plan View (OV-1_2) 11

Figure 3 - Notional CDC Logical View (OV-1_3) 12

Figure 4 - Notional CDC Functional View (OV-1_4) 13

Figure 5 - Top Level CDC Operational Activities (OV-5a) 14

Figure 6 - TIA-942 & DoD Standards Categories 16

Figure 7 - Delivering Core Data Center Enterprise Services (OV-1_5) 22

Figure 8 - High Level CDC Zone Architecture 25

Figure 9 - Defense ITIL Overview 33

Figure 10 - Node Tree Level 0 and Level 1 51

Figure 11 - Manage Facility Infrastructure Nodes 51

Figure 12 - Manage Computing Infrastructure Nodes 52

Figure 13 - Deliver Capabilities Nodes 52

Figure 14 - Ensure Security/IA Nodes 53

Figure 15 - Provide Operations & Processes Nodes 53

Table 1 - Data Center Types 10

Table 2 - Data Center Availability Tiers Summary 15

Table 3 - Facility Infrastructure Principles and Rules (OV-6a/1) 16

Table 4 - Computing Infrastructure Principles and Rules (OV-6a/2) 19

Table 5 - Capability Delivery Principles and Rules (OV-6a/3) 23

Table 6 - Security/IA Principles and Rules (OV6a/4) 28

Table 7 - Operations & Processes Principles and Rules (OV-6a/5) 33

Forward

This is a modified version of the CDC RA v1.0. Certain content has been redacted to allow it to be publically released. The un-redacted version is available to those with an account on the unclassified Intelink fabric at the following url:

<https://www.intelink.gov/sites/dodfdcci/default.aspx>

Executive Summary

The Core Data Center Reference Architecture (CDC RA) prescribes the required characteristics for the set of highly capable, highly resilient and standardized Enterprise data centers that will form the backbone of the Joint Information Environment (JIE) computing infrastructure now being implemented. These CDCs will be selected from existing DoD data centers and will host both Enterprise and Component-unique services including DoD Cloud Computing services. Core Data Centers will enable a significant reduction in the total number of DoD data centers by serving as consolidation points for computing and storage services currently hosted across hundreds of Component facilities.

The CDC RA v1.0 is intended to be used by the DoD Components to help identify candidate CDCs, and once selected, to guide detailed design and planning activities for those facilities. In the near-term, the CDC RA v1.0 will also be used to inform POM 15 funding decisions. Longer-term, the CDC RA will be used to help establish DoD guidelines for wider scale use of commercial data centers and hosting services in support of law and Federal mandates.

The CDC RA v1.0 establishes required characteristics for CDCs in the form of principles, rules, standards and other architectural patterns. These requirements are divided into five areas: facility infrastructure, computing infrastructure, security/information assurance, capability delivery, and standardized operations and processes. These requirements were derived from multiple DoD and industry sources and shaped through a collaborative process involving the DoD Architecture & Standards Review Group, the DoD Data Center Consolidation & Cloud Computing Working Group, JIE Capability Working Groups, the Deputy DoD CIO for Cyber Security, and other DoD stakeholders.

The CDC RA is part of the family of architectures that are components of the DoD Information Enterprise Architecture, the capstone architecture for the Enterprise Information Environment Mission Area (EIEMA). It is developed to convey Enterprise level technical direction to meet JIE and EIEMA goals.

1.0 Strategic Purpose

1.1 Introduction & Overview

1.1.1 Purpose

This reference architecture defines the required attributes of DoD Core Data Centers in the target objective state (~2017/2018). It is intended to guide the implementation of a set of agile, highly capable and standardized fixed computing facilities that will deliver DoD IT Services to all authorized DoD users in a manner optimized for performance, efficiency and security. The CDC RA will serve as a primary source of guidance for Component solution architectures and programs necessary to achieve the Computing Infrastructure vision of the JIE) and will be used to assess compliance of CDCs to established standards.

1.1.2 What Is a Core Data Center?

DoD computing and data storage facilities in the target state (~2017/2018) have been categorized into four types: Core Data Centers (CDC), Installation Processing Nodes (IPN), Special Purpose Processing Nodes (SPPN), and Tactical/Mobile Processing Nodes (TPN). The JIE vision is that all current data centers will either close or transition to one of these four types. CDCs will be the most robust and capable data centers in the inventory. They will be the preferred provider for all enterprise-wide computing and data storage capabilities as well as non-enterprise (Component) computing and data storage capabilities. CDC's are marked by the following key attributes:

- Each CDC is operated by a Component (Combatant Command, Military Service, or Defense Agency) under a “franchise”¹ model. In the future, commercially operated CDCs may be included
- Standardized operations, processes and governance managed by the Global Operation Center and regional Enterprise Operation Centers being developed by JIE
- Fixed/permanent facilities meeting TIA-942 and Uptime Institute Tier III standards and DoD requirements for critical infrastructure
- Highly resilient and secure through redundant infrastructure, multiple, robust bandwidth connections to the DISN core backbone, and co-location with Enterprise-managed network security boundaries and Internet Access Points
- Hosting of non-Intelligence Community Enterprise services and applications
- Provide co-location/hoteling for non-Intelligence Community DoD Component services and applications
- Regional content staging, disaster recovery, COOP, and archiving for other CDCs and other data center types
- Computing and storage capacity able to support Enterprise cloud computing and server virtualization technologies

¹ Under the franchised model each CDC might be operated by a different DoD organization but all CDCs will be subject to the same DoD Enterprise governance and would be standardized in terms of facility, technology and operations. The franchise model will be developed in greater detail in future guidance to be developed by JIE.

- Scalable space, power, and infrastructure
- Host and operate designated portions of the DoD Cloud Platform now being developed

Core Data Centers will be selected from existing Component data centers based on this reference architecture and other criteria being developed by the DoD CIO in coordination with the ITESR/JIE effort and the Components. Version 1.0 of the CDC RA focuses primarily on CDCs; future guidance will address the other data center types.

1.1.3 Derivation of Content

The requirements for CDCs as expressed in the principles, rules, patterns and standards were distilled from various sources. These sources included existing data center guidance provided by DoD CIO, DISA and the Military Services, readily available industry standards and best practices, and input from various working groups. The draft requirements were coordinated with the Components through the DoD Architecture & Standards Review Group, the DoD Data Center Consolidation & Cloud Working Group, and the JIE Capabilities Working Group. More than 600 comments were received during the coordination phase. CDC RA Version 1.0 reflects the agreed to adjudications of those comments.

1.2 Scope, Assumptions, Constraints and Intended Audience

1.2.1 Scope

Version 1.0 of the CDC RA is scoped around the characteristics required to standardize CDCs. It addresses:

- A target state (to-be) perspective (~2017/2018) aligned with the JIE vision for DoD computing
- DoD Enterprise level technical direction in the form of principles, rules and standards for defining CDCs in five categories: facility infrastructure, computing infrastructure, capability delivery, security/information assurance, and standardized operations and processes
- High level capability and operational perspectives related to the future JIE computing environment and CDCs
- Terms and definitions related to CDCs and other data center types

1.2.2 Assumptions & Constraints

Key assumptions and constraints that underlie Version 1.0 of this reference architecture:

- DoD direction on data centers, data center consolidation, cloud computing, and server virtualization is evolving. This RA will be developed iteratively with each successive version incorporating new or matured guidance
- This RA is not intended to serve as a means to establish the basis for adoption of cloud computing in DoD but instead points the reader to the approved DoD Cloud Computing Strategy (July 2012)
- This RA is only one part of a larger set of guidance that will be developed to guide the Department to the vision of the JIE target state

- This RA serves as Enterprise-level direction for the development of lower-level architectures, engineering designs, acquisitions, and related programs
- The scope of CDC operations does not include the delivery of TS/SCI services and applications for the Intelligence Community (IC); however, DoD CIO and JIE have engaged with the IC CIO to explore future collaboration
- This RA as an element of the DoD Information Enterprise Architecture (IEA) Version 2.0 in and specifically supports the JIE vision for the DoD Computing Environment
- This reference architecture does not supersede law or DoD policy. Specifically, it will not impact the special needs of the U.S. Special Operations Command as codified in USC 10 Section 167

This version of the CDC RA will not address:

- Requirements/standards for other types of data centers in the JIE target state (IPNs, SPPNs, TPNs)
- CDC governance, CONOPs, performance management, or implementation of the target state environment
- Engineering or solution level technical guidance
- Requirements for CDC operator or maintainer training
- Individual enterprise services or service delivery details
- Details on standardized operations and processes including process models or flow charts

1.2.3 Intended Audience and Uses

The CDC RA is intended to be used by the Military Departments, Combatant Commanders, DISA and other Defense Agencies that operate existing DoD computing facilities to aid in the identification and implementation of CDCs that will operate according to the principles, rules and standards contained in this RA. It serves as the Enterprise-level technical direction for the development of Component-level solution architectures, engineering designs and related planning, programming, budget and acquisition activities. It will assist Components in making decisions by providing a means to assess existing data centers against CDC criteria. Existing data centers determined not to be a candidate CDC will be further evaluated for potential consolidation with a CDC and transition to one of the other target state data center types or closed.

1.3 Alignment with the Joint Information Environment

The JIE vision is “a robust and resilient enterprise that delivers faster, better informed collaboration and decisions enabled by secure, seamless access to information regardless of computing device or location.”² JIE is comprised of IT capabilities, operations and defense of those capabilities, and overall governance. The CDC RA has been developed in coordination with the JIE initiative and is aligned with the JIE capabilities for the future computing infrastructure. The JIE initiative has identified this reference architecture in their planning documentation as a primary authoritative source for establishing CDCs. The CDC RA is;

² JIE Overview Materials – April 2012

however, just one part of a larger set of guidance that will be required to enable the future DoD Computing Environment envisioned by the ITESR and JIE. This additional guidance includes architectures, CONOPs, transition plans, and technical direction addressing cloud computing, virtualization, and tactical/mobile computing among others. The DoD CIO will continue to coordinate with JIE to ensure all necessary guidance is developed.

1.4 Architecture Development

The development of this reference architecture follows standard DoDAF v2.0 practices and conforms to its conventions as well as DoD IEA compliance requirements and the DoD Reference Architecture Description document. Data collected was used to populate DoDAF models, which were then used to build this integrated architecture report. Section 1.0 (this section) provides an introduction and overview of the CDC RA and is populated from the AV-1 view. Section 2.0 defines the high-level Operational and Capability Viewpoint perspectives that establish the vision and goals for data center consolidation/optimization in DoD and the role of the CDC RA in that vision. This section is populated from the OV-1 and CV-1 views. Section 3.0 identifies the required attributes of CDCs in terms of principles, rules and patterns with the information presented in a set of tables aligned to the high level OV-5a node tree. It is populated from the OV-5a and OV-6a views. Appendix A provides the detailed version of the AV-1 Overview & Summary. Appendix B is the listing of the relevant standards (StdV-1). Appendix C is the Operational Activity node tree (OV-5a). Appendix D is the Glossary & Integrated Dictionary (AV-2).

The DoD IEA and subordinate reference architectures (including this reference architecture) can be found at: <https://www.intelink.gov/sites/dodieav2/default.aspx>. (Intelink account required).

2.0 The Vision for Computing Transformation in the Department

2.1 Overview and Problem Statement

The Department of Defense currently has more than 1,000 fixed³, non-tactical, data centers across the world operated by the Military Departments, Combatant Commands, DISA, and other DoD Components. These data centers range from large dedicated sites delivering DoD Enterprise-wide services (e.g., DISA DECCs) to installation-level server rooms supporting individual base/post/camp/station facilities. Collectively, these data centers form the part of the DoD Information Enterprise responsible for data storage, information processing, and delivery of designated services (infrastructure, platform and software).

These data centers were largely developed around individual needs of the parent organization or program office without significant regard for interoperability, standardization, efficiency, or the ability to migrate to newer technologies. Key shortcomings of the current set of data centers include:

- Taken as a whole, the physical and computing capacity of DoD data centers is not optimized resulting in wasteful resource utilization
- Program-specific data centers that build and manage their own hardware, software, platforms, and applications are expensive, inefficient, non-interoperable, and in-flexible
- Enterprise-level services are not effectively provided to bandwidth limited or disconnected users in the tactical environment
- Disparate data repositories and access methods increase the amount of time necessary to obtain information needed to adapt to changing environments and enable tactical and strategic decisions based on cohesive and relevant information
- Lack of standardization across data centers in the way services are delivered to users and internal business operations is inefficient and make it difficult to assess the true total cost of ownership (TCO) of an IT system
- The sheer number of data centers and networks are not effectively managed as a single enterprise creating unnecessary security risks; inconsistent implementation of security and IA controls in legacy data centers
- Inability to easily and quickly adapt to new technologies and service delivery mechanisms such as cloud computing and server virtualization

2.2 Transformational Vision and High Level Goals

The overall vision for the future DoD computing environment is the ability to deliver a standardized, agile, and ubiquitous set of computing capabilities available to all authorized users as part of a services-based Information Enterprise (IE). Computing and storage services will be delivered through a set of consolidated and interconnected Core Data Centers, Installation Processing Nodes, Special Purpose Processing Nodes, Tactical/Mobile Processing

³ Fixed refers to a permanent or semi-permanent, non-mobile, structure

Nodes, and end-user devices that deliver cloud-based, on demand services while also continuing to support existing/legacy services and applications. The high-level goals are:

- Significantly reduce the number of DoD data centers in support of the Federal Data Center Consolidation Initiative and the DoD IT Enterprise Strategy & Roadmap.
- Reduce excess hardware infrastructure in data centers by adopting virtualization technology and reducing the number of instances of multiple applications
- Reduce software redundancy and rationalize the software infrastructure through the implementation of standardized software platforms (including cloud platforms) that are continuously monitored and respond to emerging threats
- Make common applications and services (e.g., email, collaboration) available to all DoD users that are secure, highly scalable, and can be rapidly configured and deployed
- Ability to provide on-demand capacity and self-provisioned services that can scale, as required, to user needs
- A federation of “franchised” CDCs, IPNs, SPPNs, and TPNs with robust interconnectivity and global accessibility delivering services to all authorized users in all locations
- Authorized users can access needed information from anywhere from any authorized device. Data is visible, accessible and understandable based on security privileges
- Improved security posture and agility (ability to recover from unplanned events) of the computing infrastructure
- Ability to more readily adopt emerging commercial technologies, platforms and services

2.3 Support for Legal and Regulatory Mandates

2.3.1 Federal Data Center Consolidation Initiative (FDCCI)

Under FDCCI, the DoD has committed to a goal of 428 data centers by the end of FY15. This represents a reduction of over 40% from the FY10 baseline level of 772 data centers. This is a first step, even more aggressive consolidation of data centers must be pursued to achieve overall IT efficiency and performance targets. Significant consolidation can only be achieved by:

- Reducing the duplication of services and applications hosted in data centers by transitioning to cloud-based delivery mechanisms
- Standardizing the delivery of core enterprise services and applications from CDCs
- Using CDCs to the maximum extent possible for providing all other DoD computing needs to achieve economies of scale⁴
- Transitioning legacy services and applications to run in virtualized environments thereby reducing the number of physical servers that are needed

The CDC RA is one part of the solution. In particular, it establishes the required characteristics for CDCs and establishes the foundation for the implementation of cloud computing technologies.

⁴ Unlike most public and private sector organizations, the number, location, and functions of DoD data centers cannot be assessed strictly on cost or performance considerations. The unique Warfighting mission of the DoD must also be considered in determining requirements for computing, storage and service delivery needs.

2.3.2 FY12 National Defense Authorization Act (NDAA)

NDAA Section 2867, *Data Servers and Centers*, requires in part that the Department develop a Performance Plan for: (1) reducing data centers and related IT, (2) increasing multi-organizational use of data centers and IT services, and (3) a finite set of metrics to report on data center infrastructure. The FY12 NDAA also establishes new authority for the DoD CIO in certifying that DoD Component data center acquisitions meet the approved Performance Plan. The CDC RA provides the approved standards for CDCs necessary to enable large scale multi-organizational use of data centers, through standardization enable data center consolidation and closures, and it provides a mechanism for assessing proposed acquisitions related to CDCs against the approved Performance Plan.

2.4 The JIE Computing Infrastructure

The types of data centers that exist today as well as the four types of data centers that will exist in the JIE target state of 2017/2018 and their descriptions is shown in Table 1.

Today	JIE 2017/2018	Description
DISA Enterprise Computing Centers (DECCs) Component Enterprise Data Centers	DoD Core Data Center (CDC)	A fixed DoD data center meeting DoD standards for facility and network infrastructure, security, technology, and operations and adhering to enterprise governance under a “franchise” model. Functions and services delivered by current DISA DECCs, Component Enterprise DCs and Component Installation DCs will be consolidated to the greatest extent possible into Core DCs totaling a few dozen at most. CDCs will be selected from existing Component data centers.
Component B/P/C/S Installation Data Centers	Installation Processing Node (IPN)	A fixed DoD data center serving a single DoD installation with local services that cannot be (technically or economically) provided from a CDC. There will only be one IPN per DoD installation but each IPN may have multiple enclaves to accommodate unique installation needs (e.g., Joint Bases).
Component Functional & Special Purpose Data Centers	Component Special Purpose Processing Node (SPPN)	A fixed data center or data servers in a fixed facility supporting special purpose functions that cannot or should not be supported by Core DCs or IPNs due to its association with mission specific infrastructure or equipment (e.g., Meteorology, Medical, Modeling & Simulation, Test Ranges, Classrooms, RDT&E, etc.).

Today	JIE 2017/2018	Description
Component Tactical/ Mobile Data Centers	Component Tactical/Mobile Processing Node (TPN)	Tactical/Mobile Processing Nodes of the target state will provide services very similar to those of fixed Core DCs but are optimized for the tactical environment or deployable computing needs. TPNs will connect to the JIE network whether in garrison or deployed, but may do so in different ways (e.g., terrestrial fiber vs. satellite connectivity).

Table 1 - Data Center Types

All existing data centers in the DoD inventory will transition to one of these four types of data centers or will be closed over the next 5 – 7 years. The number and location of each data center in the target state and the services each provides will be optimized to meet all computing requirements of the DoD JIE and all Warfighting requirements for computing. These parameters are not specified in this RA but will be determined through other data center transformation initiatives currently underway.

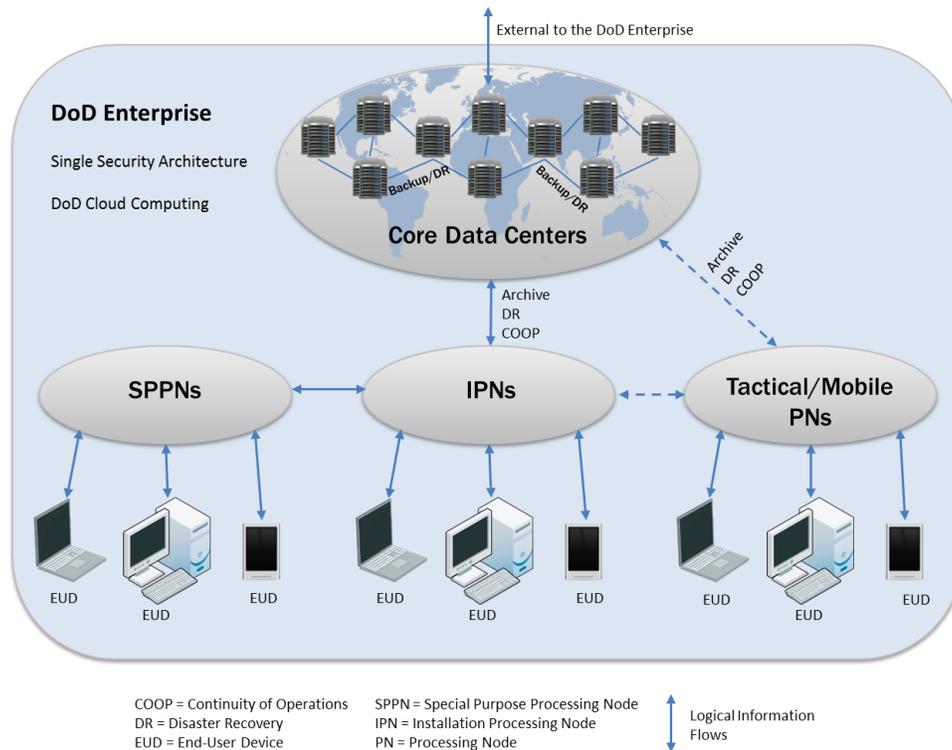


Figure 1 - DoD Enterprise Perspective (OV-1_1)

Figure 1 depicts these target-state data centers graphically as part of the future DoD Computing Enterprise as defined by JIE. This Enterprise includes the data centers, the end-user devices, the users (not shown) and the data itself (not shown) all logically tied together through the JIE Network and JIE Single Security Architecture. Components of the DoD cloud platform will be installed at each of these nodes to provide the end-to-end delivery of cloud-based services. The CDCs are the focus of this RA. Details on the other data center types, their interfaces to

the CDCs and each other will be published in future guidance. Current direction from the Office of Management and Budget on moving toward greater sharing of IT services across all levels of government may result in future change to the way some DoD data and IT services are managed. Table 1 and Figure 1 do not address DoD IT services delivered from non DoD-owned data centers (some are today) but will be updated in the future as the Department evolves plans for addressing these Federal mandates.

2.5 Functional Perspective

Figure 2 is a notional floor plan view of a CDC. It conveys one of the key functional requirements of a CDC as a provider of both newer cloud-based services as well as a provider of existing legacy services. The cloud and legacy delivery models will support both DoD Enterprise Services and Component-unique services. Figure 2 also depicts several themes addressed later in the document including infrastructure redundancy, dedicated build and staging spaces, and segregation of climate and security zones.

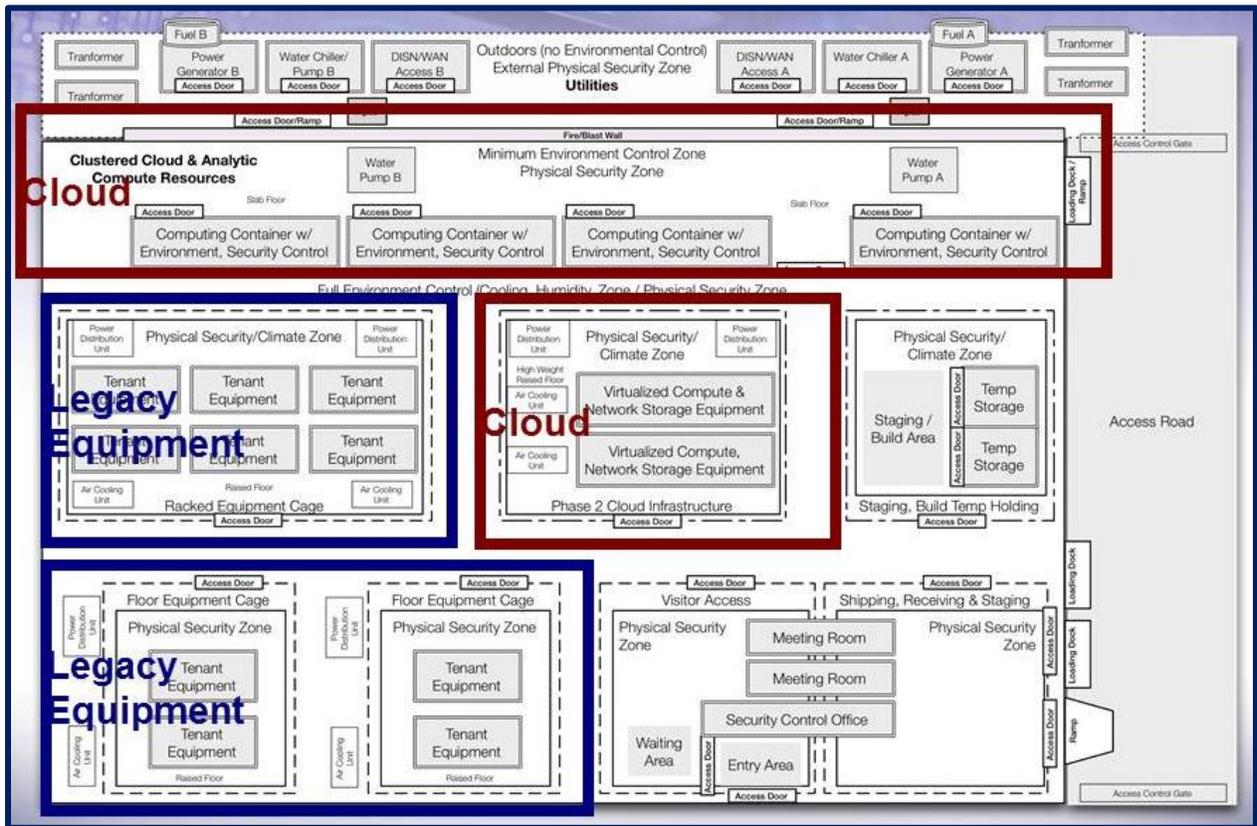


Figure 2 - Notional CDC Floor Plan View (OV-1_2)

Figure 3 is a notional logical view of the CDC. It highlights several CDC requirements including:

- CDC connectivity (in green on the far right of the figure) including NIPRNET, SIPRNET and JWICS

- CDC internal support functions (in blue on the middle right) including provisioning, monitoring, and cost recovery
- Support for multi-tenancy (middle in light blue)
- CDC Management functions (in blue across the top)

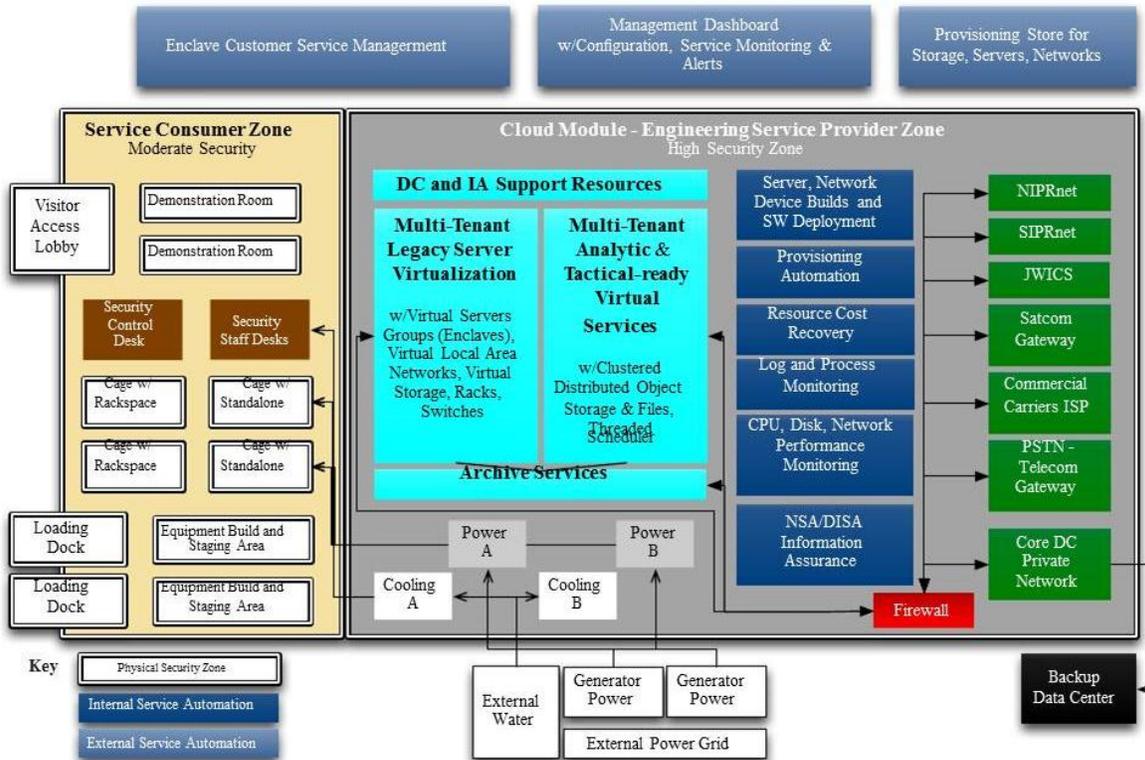


Figure 3 - Notional CDC Logical View (OV-1_3)

Figure 4 is a notional functional view of the CDC from the cloud-delivery perspective. The output of the conceptual CDC environment leverages the physical computing infrastructure to deliver data and cloud services to the user, regardless of access point or the device being used. Mechanisms for the delivery of these services include Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). Attributes relating to the delivery of services expressed as principles, rules and standards can be found in Section 3.0.

While franchised CDCs may be operated by different organizations within DoD, they will all operate according to a set of standard operational, business, and IT Service Management processes. This is shown in the cylinder on the right in Figure 4. This is particularly important to ensure that all CDCs function as a single, logically seamless computing environment meeting all requirements for seamless fail over, disaster recovery, continuity of operations, and load balancing. Customers of CDCs will expect to have the same experience and to interact in similar ways irrespective of the particular CDCs from which they are receiving services.

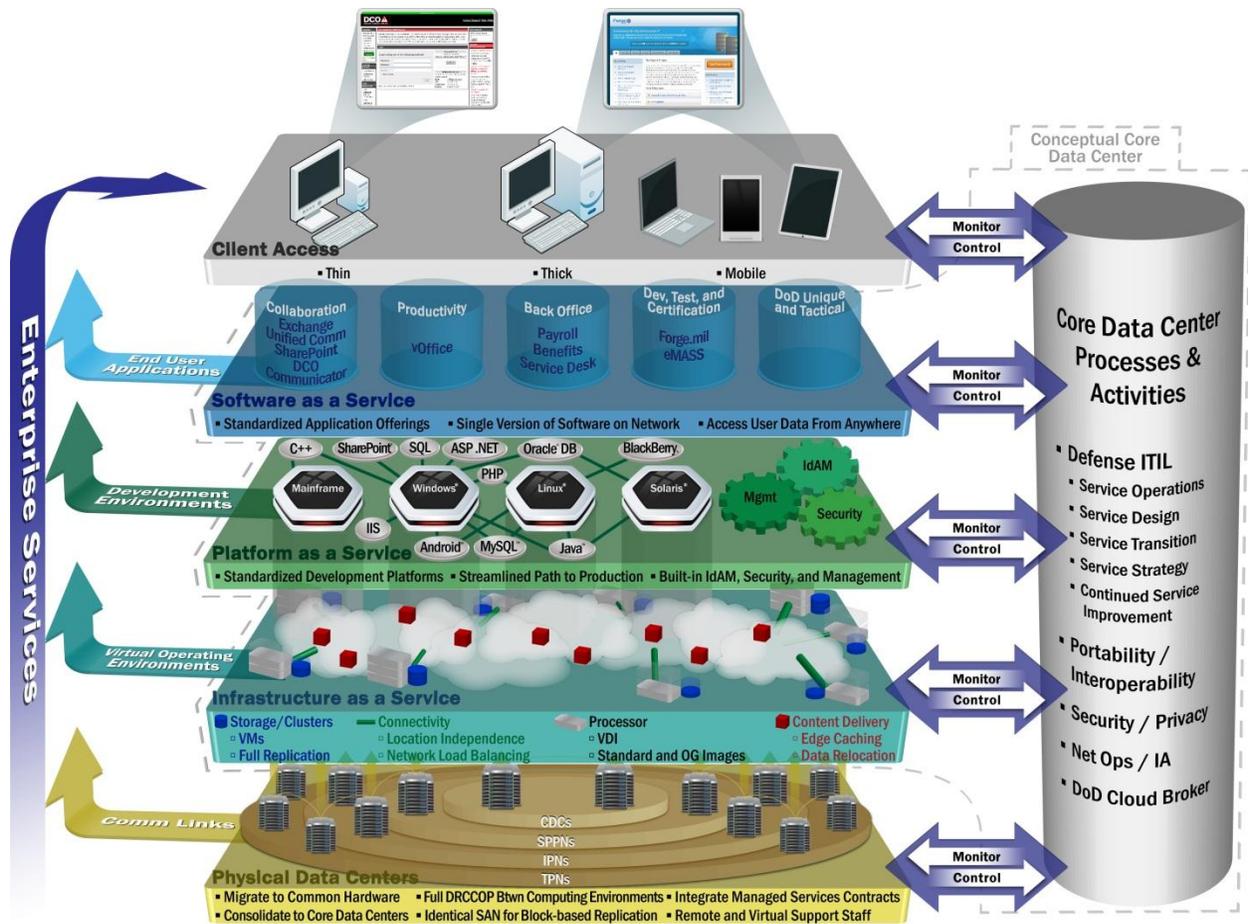


Figure 4 - Notional CDC Functional View (OV-1_4)

3.0 Core Data Center Requirements

The primary focus of this document is to define the minimum requirements needed to guide the development of engineering-level solutions and related tasks for the implementation of CDCs. These requirements are expressed as principles, rules and standards and divided into the following five categories:

- Facility Infrastructure (Section 3.1)
- Computing Infrastructure (Section 3.2)
- Capability Delivery (Section 3.3)
- Security/Information Assurance (Section 3.4)
- Standardized Operations & Processes (Section 3.5)

Each category is addressed in Sections 3.1 through 3.5 and is organized into an overview of the category providing background and context followed by a table of the relevant principles and rules. Appendix B contains descriptive Information on the DoD and industry standards that are called out in the rules.

These categories also serve as the basis for a related set of operational activities that define the CDC in terms of the key, operationally-focused outcomes. The operational activities are structured in a parent/child node tree organization with each successive level in the tree containing sub activities of greater detail. This node tree will be used as the basis for building standardized process models in future versions of this reference architecture. The top two levels of the node tree are shown in Figure 5. The complete model can be found in Appendix C.

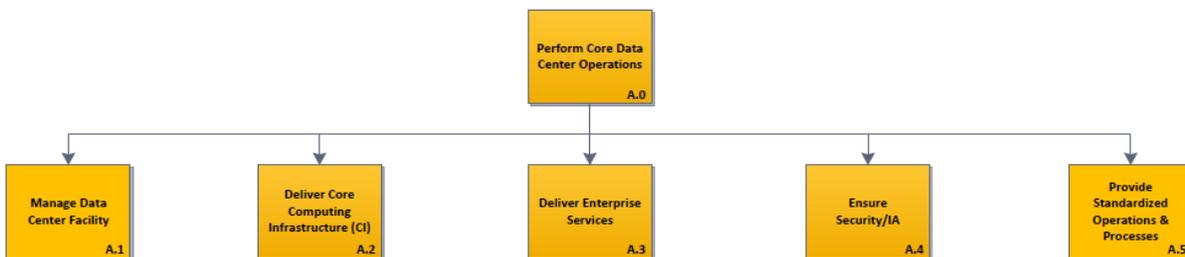


Figure 5 - Top Level CDC Operational Activities (OV-5a)

3.1 Facility Infrastructure

3.1.1 Overview

The physical infrastructure of a CDC must be highly reliable and resilient in order to support uninterrupted service, or “uptime,” to mission critical computing, data processing and communications operations. TIA-942 (including addendums⁵), *Telecommunications Infrastructure Standard for Data Centers*, is a widely adopted industry standard providing

⁵ The TIA-942 basic edition of Apr 2005 has two addendums, TIA-942-1 (Mar 2008) and TIA-942-2 (Mar 2010). TIA has announced plans to issue a completely revised 2012 edition but has not done so as of the publication date of this reference architecture.

UNCLASSIFIED

requirements and guidelines for data center facility design. The Uptime Institute⁶ has published a companion standard, *Data Center Site Infrastructure Tier Standard: Topology*, which establishes four data center tiers (I – IV). Each successive tier represents a higher level of data center availability based on increased redundancy of the facility components described in TIA-942. Greater redundancy and spare capacity increases the statistical availability figure for data center capability delivery but almost always does so at increased costs. Striking the right balance between availability and cost is a key concern of data center designers. A summary of the tiered requirements is depicted in Table 2.

	Tier I	Tier II	Tier III	Tier IV
Active Capacity Components to Support the IT Load	N	N+1	N+1	N After any Failure
Distribution Paths	1	1	1 Active and 1 Alternative	2 Simultaneously Active
Concurrently Maintainable	No	No	Yes	Yes
Fault Tolerance	No	No	No	Yes
Compartmentalization	No	No	No	Yes
Continuous Cooling	Load Density Dependent	Load Density Dependent	Load Density Dependent	Load Density Dependent

Table 2 - Data Center Availability Tiers Summary

The “N” in Table 2 represents the capacity figure for a facility component (e.g., cooling) needed for basic data center operations with no allowance for redundancy. For example, consider a Tier I data center that has a single 50 ton cooling unit to meet normal operational conditions. If that cooling unit fails then data center operations are disrupted. For the same data center to be Tier III compliant a second 50 ton cooling unit would be required and configured to come on line so that the first unit can be taken off line for maintenance without affecting cooling (concurrent maintainability).

This reference architecture adopts TIA-942 design requirements for CDCs and establishes Tier III as the target availability standard. This target availability standard may be upgraded to Tier IV in the future for some or all of the CDCs.

⁶ The Uptime Institute is an industry consortium whose data center tier standard has been widely adopted throughout the world as a benchmark for assessing data center availability and performance

UNCLASSIFIED

TIA-942 Facility Standards	Tier I Basic Site Infrastructure N	Tier II Redundant Site Infrastructure N + 1	Tier III Concurrently Maintainable Site Infrastructure N + 1	Tier IV Fault Tolerant Site Infrastructure 2 (N + 1)
Telecommunications Standards			CDC RA V1.0	Future
Architectural & Structural Standards			CDC RA V1.0	Future
Electrical Systems Standards			CDC RA V1.0	Future
Mechanical Systems Standards			CDC RA V1.0	Future

Additional DoD Standards Categories

DoD Critical Facility/Antiterrorism Standoff Distances Standards	DoD Cloud Standards	Network Standards
Security/IA Standards (Incl. C&E, TEMPEST, DMZ, etc.)	DoD Enterprise Services Standards	DoD Core DC Standard Operation & Process Standards

Figure 6 - TIA-942 & DoD Standards Categories

As shown in Figure 6, The TIA-942 facility requirements are divided into four groups: telecommunications, architectural & structural, electrical, and mechanical. The exemplar CDC facility will have multiple paths, one active and one passive, for both power and cooling. Each of these paths has the capacity to support the facility when the other path becomes unavailable. Tier III data centers are designed so that the removal of parts of a distribution path do not result in the loss of availability of the computing equipment. In addition to the TIA-942 requirements, CDCs will meet DoD-unique requirements for anti-terrorism protection, security and IA, cloud computing, Enterprise services, networking, and processes.

3.1.2 Principles and Rules

The facility infrastructure principles and rules are found in Table 3

Table 3 - Facility Infrastructure Principles and Rules (OV-6a/1)

Rule #	Rule Description	Supporting Rationale/Comments
Principle #1: Core Data Centers will meet widely adopted industry standards for computing infrastructure that supports Enterprise-wide services that must be continually available.		
1.	CDCs shall have a minimum of 7,500 sq ft (CONUS) or 4,000 sq ft (OCONUS) of raised deck computing floor space or equivalent floor space served by overhead cable tray	DoD CDC Selection Criteria per the DoD CDC Selection WG
2.	CDCs (CONUS & OCONUS) shall have a minimum of 1,000 sq ft of available (excess) raised deck computing floor space or equivalent floor space served by overhead cable tray	DoD CDC Selection Criteria per the DoD CDC Selection WG
3.	CDCs shall at a minimum meet the Tier III facility availability criteria and system redundancy requirements.	Uptime Institute Tier Topology Standard and TIA-942
4.	CDCs shall provide at least "N+1" levels of	Uptime Institute Tier III

UNCLASSIFIED

Rule #	Rule Description	Supporting Rationale/Comments
	redundancy for all electrical and mechanical subsystems (<i>"N" being systems required for normal operations and "+1" being spare capacity</i>)	TIA-942
5.	CDCs shall have at least two diversely routed delivery paths for commercial electrical power with one active path and one passive (standby) path. Each electrical feed will be delivered at medium voltage (600 volts) or higher.	Uptime Institute Tier III TIA-942
6.	CDCs will be served by at least two commercial or DoD power generation stations.	DoD CDC Selection Criteria per the DoD CDC Selection WG
7.	The CDC facility shall be equipped with N+1 prime rated generator units	Uptime Institute Tier III TIA-942
8.	CDCs shall have at least 0.5 MW of available (excess capacity) electrical power	DoD CDC Selection Criteria per the DoD CDC Selection WG
9.	Upon loss of electrical power from the primary source for a given CDC, electrical power is restored to key IT assets by automatically activated power generators on site.	This control is satisfied by the site and a system cannot satisfy the requirement.
10.	CDCs shall support the ability of external providers of power and communications services to access external connections and to test/monitor delivery of services	
11.	Air conditioning systems shall be designed to run 7/24/365 with at least +1 redundancy to the units that are cooling the computing infrastructure. All temperature control systems should be powered by dedicated electrical circuits to ensure optimal temperature ranges are always maintained.	Uptime Institute Tier III TIA-942
12.	CDCs shall have at least 72 tons of available (excess) HVAC capacity	DoD CDC Selection Criteria per the DoD CDC Selection WG
13.	CDCs shall use outside (free) air cooling where appropriate.	
14.	CDCs shall be routinely audited for compliance by an accredited, independent 3rd party organization	To be developed as part of JIE implementation
15.	CDCs shall support standard loading/unloading docs, pallet unloading/loading, package storage, equipment staging and egress security.	
16.	All CDC IT hardware shall be secured in enclosed racks	This control is satisfied by the site and a system cannot satisfy this requirement.
Principle #2: Core Data Centers will be designated as DoD critical infrastructure assets and meet applicable requirements.		
17.	CDCs shall be designated as DoD critical infrastructure assets per governing policy	DoD Manual S-3020.45 Volume 4, "Defense Critical Infrastructure Program (DCIP): Defense Critical Asset (DCA) Nomination and Submission Process (U)", March 20, 2009
18.	CDCs shall meet critical infrastructure requirements for site planning, structural design, architectural design and electrical and mechanical design	UFC 4-010-01 UFC 4-010-02
19.	CDCs shall meet minimum infrastructure requirements for anti-terrorism minimum stand-off distances	UFC 4-010-02

Rule #	Rule Description	Supporting Rationale/Comments
Principle #3: Core Data Centers will meet applicable DoD, Federal, and local building codes including but not limited to the following:		
20.	An automatic emergency lighting system is installed that covers all areas necessary to maintain mission or business essential functions, to include emergency exits and evacuation routes.	This control is satisfied by the site and a system cannot satisfy the requirement.
21.	Battery-operated or electric stand-alone smoke detectors are installed in the facility.	This control is satisfied by the site and a system cannot satisfy the requirement.
22.	A servicing fire department receives an automatic notification of any activation of the smoke detection or fire suppression system.	This control is satisfied by the site and a system cannot satisfy the requirement.
23.	Computing facilities undergo a periodic fire marshal inspection. Deficiencies are promptly resolved.	This control is satisfied by the site and a system cannot satisfy the requirement.
24.	Handheld fire extinguishers or fixed fire hoses are available should an alarm be sounded or a fire be detected.	This control is satisfied by the site and a system cannot satisfy the requirement.
25.	A fully automatic fire suppression system is installed that automatically activates when it detects heat, smoke, or particles.	This control is satisfied by the site and a system cannot satisfy the requirement.
26.	Humidity controls are installed that provide an alarm of fluctuations potentially harmful to personnel or equipment operation; adjustments to humidifier/dehumidifier systems may be made manually.	This control is satisfied by the site and a system cannot satisfy the requirement.
27.	Automatic humidity controls are installed to prevent humidity fluctuations potentially harmful to personnel or equipment operation.	This control is satisfied by the site and a system cannot satisfy the requirement.
28.	A master power switch or emergency cut-off switch to IT equipment is present. It is located near the main entrance of the IT area and it is labeled and protected by a cover to prevent accidental shut-off.	This control is satisfied by the site and a system cannot satisfy the requirement.
29.	Automatic temperature controls are installed to prevent temperature fluctuations and provide an alarm when fluctuations become potentially harmful to personnel or equipment; adjustments to heating or cooling systems may be made manually.	This control is satisfied by the site and a system cannot satisfy the requirement.
30.	Automatic temperature controls are installed to prevent temperature fluctuations potentially harmful to personnel or equipment operation.	This control is satisfied by the site and a system cannot satisfy the requirement.
31.	Automatic voltage control is implemented for key IT assets.	This control is satisfied by the site and no one system cannot satisfy the requirement.
Principle #4: Core Data Centers will be connected to diversely routed, high capacity (bandwidth) wide area network nodes.		
32.	CDCs will be served by at least two (2) redundant and diversely routed fiber WAN connections to the DISN	DoD CDC Selection Criteria per the DoD CDC Selection WG
33.	Each CDC WAN connection shall be at least 10 Gbps in bandwidth (near-term FY14) increasing to 40 Gbps (longer-term FY15+)	DoD CDC Selection Criteria per the DoD CDC Selection WG
34.	CDCs must be connected to the Global Information Grid with direct access to NIPRNET, SIPRNET, JWICS, and the Internet.	DoD CDC Selection Criteria per the DoD CDC Selection WG

3.2 Computing Infrastructure

3.2.1 Overview

Core Data Centers will serve as the primary mechanism by which computing and data storage services will be made available to DoD and other authorized users. CDCs will support newer service delivery models such as cloud computing as well as legacy delivery models and do so for both Enterprise Services and Applications and approved Component Services and Applications for all mission areas. As such, CDCs must have a robust, multi-faceted computing infrastructure configured and managed to support a global user-base with on-demand capabilities that are always available. The computing infrastructure of all CDCs will be standardized to the greatest extent possible. However, some differences will exist to account for differences in the mix of Enterprise and Component services that each CDC will deliver. It is outside the scope of this reference architecture to identify which services will be delivered from a particular CDC.

A complete technical reference model identifying the specific, approved hardware, software, and storage technologies that CDCs must support is outside the scope of this version of the CDC RA but will be developed in the future. Table 4 does however identify certain technologies and should be used for assessing candidate Core Data Centers.

Virtualization technology should be at the center of Core Data Centers operations. Virtualization allows for multiple computer loads (i.e., operating systems) to run on a single physical host. Physical servers can be consolidated within virtual environments by ratios of as much as 20:1. This allows for clusters of tens of physical hosts to run hundreds of virtualized operating environments. Virtual networking between the virtual machines, the hypervisor and the physical hardware network is configured and managed within the virtualization management infrastructure. The virtual infrastructure must be able to accommodate virtual hosts running various operating systems in order to host legacy workloads.

3.2.2 Principles and Rules

Computing Infrastructure principles and rules are found in Table 4.

Table 4 - Computing Infrastructure Principles and Rules (OV-6a/2)

Rule #	Rule Description	Supporting Rationale/Comments
Principle #1: Core Data Centers will support DoD Cloud Computing delivery models as well as delivery of existing (legacy) Component services and applications. Not every CDC will deliver every Enterprise and Component service.⁷		
1.	CDC computing infrastructure shall support IaaS, SaaS, and PaaS capabilities for developers and end users.	DoD Cloud Computing Strategy
2.	CDCs shall utilize shared, virtualized infrastructure and, to the extent possible, each application will be	

⁷ The determination as to which CDCs will host/deliver a particular service or application (Enterprise or Component) will be made by the JIE operations entity and will be documented in an appropriate CONOPs (TBD)

UNCLASSIFIED

Rule #	Rule Description	Supporting Rationale/Comments
	deployed so as to consume Infrastructure-as-a-Service.	
3.	CDCs shall provide system management and administration services, system security, and system monitoring services for enterprise-class business systems in accordance with negotiated Service Level Agreements (SLAs)	
4.	CDCs shall deploy the approved DoD Cloud Platform technology independent of specific mission programs	DoD Cloud Computing Strategy
5.	CDCs shall support all technologies required to host applications approved for transition from other data centers.	DoD CDC Selection Criteria per the DoD CDC Selection WG
Principle #2: Core Data Centers will implement separate physical security and climate zones within the computing center for the following functions:		
6.	Virtualized and clustered computing equipment for multi-tenant cloud & analytic infrastructure.	Security best practices
7.	Containerized clustered cloud and analytic infrastructure	Security best practices
8.	Non-virtualized racked tenant equipment cages	Security best practices
9.	Non-virtualized standalone tenant equipment	Security best practices
10.	Staging, build, and temporary holding functions for equipment not part of the production environment	Security best practices
11.	Computing support functions (e.g., offices, repair shops, etc) – separate physical security zone only	Security best practices
12.	Facility support functions (e.g., generator rooms, utility closets, telecommunication) include separate physical security only, separate climate zone as needed	Security best practices
13.	Visitor access and shipping & receiving functions – separate physical security zone only	Security best practices
Principle #3: CDCs will employ standard hardware, software and storage technologies		
14.	CDC shall employ high density blades with dual power supplies and controller cards	DoD CDC Selection Criteria per the DoD CDC Selection WG
15.	CDCs shall support hardware processor/platform architectures in use within DoD data centers	DoD CDC Selection Criteria per the DoD CDC Selection WG
16.	CDCs shall support server operating systems in use within DoD data centers	DoD CDC Selection Criteria per the DoD CDC Selection WG
17.	CDCs shall only implement Type-1 (bare metal) hypervisor solutions	Security best practice
18.	CDCs shall support the following database types: <ul style="list-style-type: none"> • NoSQL • RDBMS (Relational DB Management System) 	DoD CDC Selection Criteria per the DoD CDC Selection WG
19.	CDCs shall utilize shared, fully redundant storage for each of the security zones (SIPR and NIPR) connected to the servers/computing environment by fiber or 10 GbE connections.	DoD CDC Selection Criteria per the DoD CDC Selection WG
20.	CDCs shall have the appropriate data backup systems for the various computing environments. These can be disk based or high-speed, high-capacity tape systems.	
21.	CDCs shall be IPv6 compliant and retain backward compatibility with IPv4 for support of legacy systems	

Rule #	Rule Description	Supporting Rationale/Comments
	still using that standard	
22.	CDCs shall provide application hosting via scalable, virtualized infrastructure on common software platforms to the greatest extent possible	
23.	CDCs shall employ a scalable, distributive architecture using open-standards-based protocols for the management of geographically dispersed servers	Detailed engineering level guidance to be developed by JIE
24.	CDCs shall support technologies required for backup, COOP, disaster recovery, and archival services	

3.3 Capability Delivery

3.3.1 Overview

Core Data Centers provide value to customers by enabling the delivery of capabilities in the form of IT services. Each CDC will support all three IT Service basic delivery models:

1. Hotel Services: CDCs provide power, cooling, space, physical security and other physical facility infrastructure for customer provided and managed hardware and software.

Responsibility for service delivery is shared between the CDC and the customer and documented in an SLA. Hotel services are sometimes referred to as co-location services.

2. Bare-Metal Services: In addition to hotel services described above, CDCs provide computer hardware for customer provided and managed software. Responsibility for service delivery is shared between the CDC and the customer and documented in an SLA.

3. Computing as a Service: The CDC provides the physical facility infrastructure, physical computing infrastructure, infrastructure services, software services, storage services, platform services, data services and virtual computing necessary to provide the customer with a particular set of capabilities in the form of one or more IT services. Responsibility for service delivery is with the CDC and documented in an SLA.

In addition to the way they are delivered, IT services in DoD can be categorized as either Enterprise Services or Component-specific services. Enterprise services are those capabilities provided as IT services to all or a large segment of the DoD user community. Component-specific services are those capabilities provided as IT services to a single Component or sub-Component. Core Data Centers will be designed to support both of these categories of services.

A key tenet of the JIE is that Core Data Centers will be the preferred provider of all IT services except those that for technical reasons must be delivered from local Installation Processing Nodes (e.g. print servers, local security and badging systems, VoIP controllers). It is recognized however, that even for systems that can technically be delivered by CDCs, there may be operational, security, or business reasons that would preclude delivery from a CDC. It is

expected that the vast majority of non-local IT services will be provided by CDCs (and not duplicated elsewhere) but the actual catalog of CDC services will be developed by JIE and the DoD CIO. The remainder of this overview is focused on Enterprise Services.

DoD Enterprise Services (ES) are IT capabilities that have been selected for shared use across the entire Department. These services can be grouped into four broad categories:

- (1) Enterprise Foundational Services,
- (2) Core Data Center Foundational Services,
- (3) Core Data Center Mandatory/Shared Common Services and
- (4) Mission Services⁸.

As depicted in Figure 7, Core Data Centers will support delivery of both Foundational and Mandatory/Shared Common ES including Computing, Infrastructure and Application Services. Core DCs will also deliver mission services determined to be Enterprise Services and approved for delivery by CDCs and may deliver all other mission services on behalf of one or more Components. Note that not every Core DC will host or deliver every Enterprise Service approved for the Core DCs. Current technology allows any particular service to be hosted in only a few data centers but provided to a world-wide customer base while meeting all requirements for availability and latency. The details of which Core DCs will be used to deliver any particular service will be determined by the JIE operations entity that manages all Core DC operations.

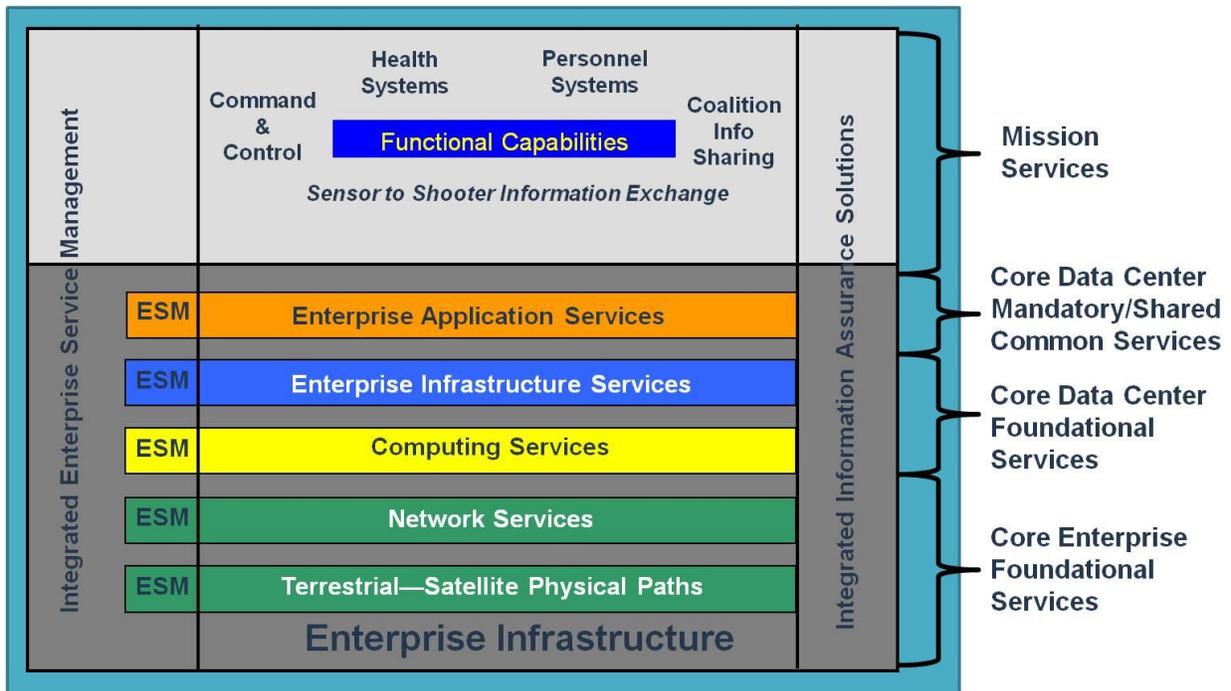


Figure 7 - Delivering Core Data Center Enterprise Services (OV-1_5)

⁸ The identification of Enterprise Services to be delivered by CDCs is under development by DoD CIO and will be reflected in future versions of this RA.

Core Enterprise Foundational Services are the ubiquitous, underlying services that enable all higher level services. These include transport, local & wide-area networks, identity, security and directory services. Core Enterprise Foundational Services are not considered Core Data Center services although some components of those services may be located at Core Data Centers.

Core DC Foundational Services provide a common set of “behind-the-scenes” infrastructure services that are critical to supporting higher-level common and shared mission services, re-usable components, and applications including: Service Catalog, Metadata Registry, IaaS, and PaaS.

Core DC Mandatory/Shared Common Services provide an enterprise-wide suite of user-facing services that satisfy end-user efficiency and interoperability requirements and include services delivered as SaaS including Enterprise E-mail, Collaboration, Unified Capabilities, Search, and Web Portal.

Mission Services are those DoD or Component-specific services and applications that support a particular mission area (Business, Warfighting, or Defense Intelligence), joint capability area, joint capability thread, or functional area. These mission services include services provided to mission partners such electronic health record information to the Department of Veterans Affairs. Figure 7 is not meant to imply that all mission services are delivered in the same way or subject to the same security controls, only that CDCs will host these services.

3.3.2 Principles and Rules

Capability Delivery principles and rules are found in Table 5.

Table 5 - Capability Delivery Principles and Rules (OV-6a/3)

Rule #	Rule Description	Supporting Rationale/Comments
Principle #1: Core Data Centers will support multiple delivery/hosting models for IT Services		
1.	CDCs shall support Hotel Services, Bare-Metal Services, and Computing as a Services as defined in this reference architecture	JIE Computing Vision
2.	CDCs shall implement and support the appropriate elements of the approved DoD Cloud Computing Platform	DoD Cloud Computing Strategy
3.	CDCs shall implement server virtualization technology to the greatest extent possible for both Enterprise and Component services	
Principle #2: Core Data Centers will be the preferred service provider for both Enterprise Services and Component-specific Services		
4.	CDCs in the aggregate shall provide all DoD Enterprise Services(approved for CDCs by JIE) to all authorized DoD and mission partner users	JIE Computing Vision
5.	CDCs shall be capable of providing Component-specific services per agreed to SLAs	JIE Computing Vision
6.	CDCs shall work with JIE network providers and the Components to ensure that Enterprise Services are provided to tactical and mobile users	JIE Computing Vision

Rule #	Rule Description	Supporting Rationale/Comments
7.	CDCs shall only host services that meet DoD approved technical, security and operational criteria	JIE Computing Vision
8.	CDCs shall publish guidelines for application/system/service developers for meeting CDC hosting criteria	
9.	CDCs shall ensure that service delivery for each service meets the availability and restoral criteria per the Mission Assurance Category and SP800-53 controls for that service	
10.	CDCs shall use COTS/GOTS solutions and other existing capabilities first, including open source solutions <ul style="list-style-type: none"> • DoD solutions will be used for military-specific needs • Customization of packaged applications will be minimized and reuse will be exploited where possible 	
11.	CDCs shall implement the approved DoD identity solutions and policy for authenticating persons and non-person entities for access to DoD computing resources	See DoDI 8520.03, FIPS 199, NIST SP 800-60 and NIST 800-122
12.	CDCs shall implement the approved DoD access management solution and policy to ensure that only users authorized to access a particular resource are able to do so	

3.4 Security and Information Assurance (IA)

3.4.1 Overview

Core Data Centers must be in the forefront of the effort to increase the Department's cyber security posture by implementing structured and integrated security, information assurance, and resiliency concepts. This approach must address a number of areas including data center zoning, secure communications, server infrastructure, identity and access management, database security, storage infrastructure, resiliency, and out of band management. Core Data Centers will be designed to meet or exceed the minimum security and information assurance standards that are outlined in the DoD 8500 Series Instructions, NIST SP800-53 Controls, and DoDI 8510.01 – Department of Defense Information Assurance Certification and Accreditation Process (DIACAP). Core Data Centers will operate under a current Authority to Operate (ATO) with current Certification and Accreditation (C&A) documentation.

Data Center Zoning

The data center must be zoned to accommodate varying levels of security access needs. Current guidance for the NIPRNet implements de-militarized zones (DMZ) at the Internet Access Points (IAP) to appropriately segment public, restricted, and private systems for the DoD. The CDCs will leverage this implementation and include additional security zones to address operational and resiliency needs. This includes a "core" computing zone which will

consist of the majority of systems residing in the CDC as well as “Specialized” and “Development & Test” zones as shown in Figure 8.

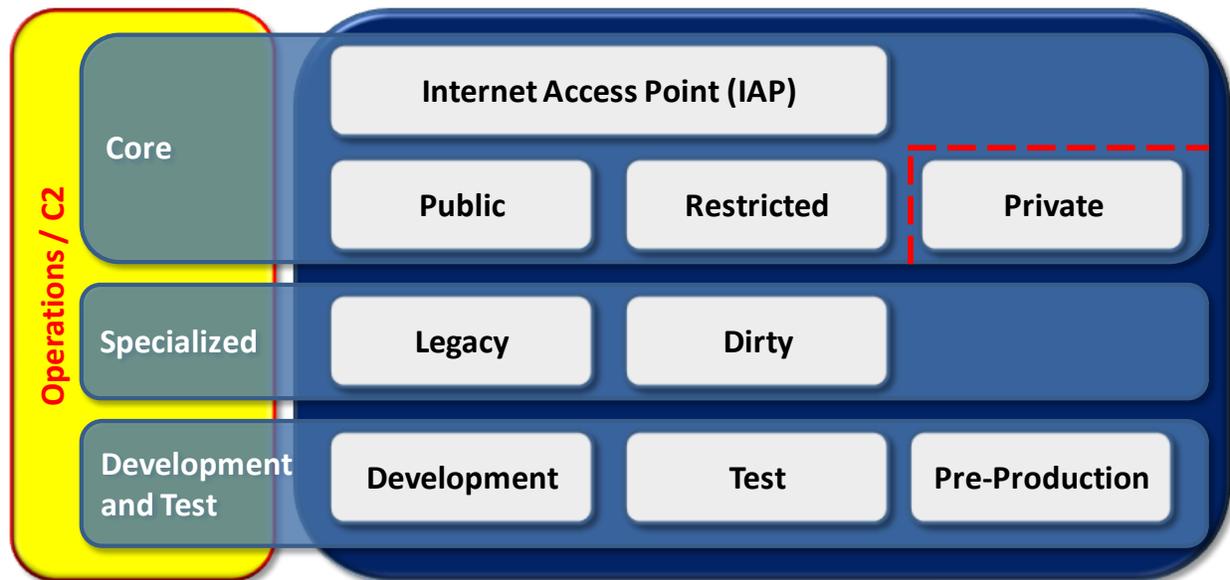


Figure 8 - High Level CDC Zone Architecture

Secure Communications

Communications within the CDC will take place among a variety of different zones. Communications between the zones will be highly protected and monitored to ensure that vulnerabilities to one zone do not compromise the other zones within the CDC. This includes encrypting traffic, internal and external to security zones, as necessary to protect the integrity of sensitive communications. A key factor for communications is that all Internet Access Points (IAPs) will be hosted within a CDC to reduce latency and provide closer management of the IAP security suite. Communication types have been divided into Intra-network communications, Inter-network communications, and Inter-CDC communications.

Intra-network communications internal to the data center environment can be categorized as follows: intra-security zone (e.g., communications internal to a single zone), inter-security zones (e.g., public to private), and inter-CDC (CDC to CDC).

Intra-security zone communications are network communications that are isolated between two machines within the same security zone. The communications security applied at this level in the CDC security architecture will include host-based security controls (specifically IPS and firewall services), network firewall and IDS/IPS devices including virtual capabilities to monitor communications internal to a virtual host and physical capabilities to monitor communications between physical hosts.

Inter-security zone communications that cross security zones in the CDC security architecture will include additional monitoring capabilities to address security communications between the sensitivity levels.

Inter-data center communications will incorporate redundant and diverse communications trunks between one (1) or more CDC(s). Connections between CDC will use dedicated, point-to-point trunks such as High Assurance Internet Protocol Encryption (HAiPE) devices with Advanced Encryption Systems (AES) -256bit encryption, FIPS 140-3 compliant devices. These devices cryptographically isolate the trunk and limit the data flow to the matched link end point. The Inter-DC trunks will additionally incorporate redundant, diverse paths from separate IAPs utilizing separate and diverse switches to avoid critical, regional and localized outages. Inter-data center communications could also traverse the DISN, depending on the load of the network utilization between the data centers.

Server Infrastructure

The security of the server infrastructure begins with hardening of the underlying support platform for the virtualized server infrastructure. Virtualization solutions in CDCs will initially be limited to type-1 (Bare Metal) hypervisor solutions. This precaution significantly reduces the risk exposure of the virtualization support platform (type -1 hypervisor vs. host OS with type-2 hypervisor) and enables the implementation and maintenance of a homogenous virtualization environment. Virtual servers will have a common STIG defined and adhered to for the security configuration of the virtual hosts. It is expected that STIGs and security requirements guides (SRGs) will be built for other virtualization platforms as part of homogeneous server infrastructure adhering to strong configuration control, management, and security.

In addition to the host security, each guest server (virtual server) will be expected to follow the standard security configuration guidance provided in the applicable DISA STIGs.

Identity and Access Management

Identity and Access Management (IdAM) includes the management of user and IT resource (i.e., servers, routers, gateways) identities and their associated roles and privileges for purposes of authenticating and authorizing access to systems and services. This includes Public Key Infrastructure (PKI) for authentication and confidentiality and Attribute Based Access Control(s) (ABAC) for authorization services.

Both user and machine authentication will leverage the current DoD PKI solution and all digital certificates will comply with the ITU-T X.509 standard. ABAC will evaluate authorization requests and enforce access decisions. All CDCs will employ eXtensible Access Control Markup Language (XACML) compliant technologies for ABAC implementation. In addition, object access control lists (ACLs) will be replaced with Policy Decision Point (PDP) logic that will evaluate attributes provided by requesters relative to established policies to make access decisions. This will alleviate the need for a repository of users, resources and their associated controls and reduce management and administrative overhead. CDC(s) will implement a DoD-wide metadata framework to include attributes such as citizenship, organization, and geographic location and associated policy-based data such as actions, environments, functions, and conditions to make decisions for ABAC implementation.

From an architectural perspective, each CDC will include at least one Certificate Distribution Point (CDP), Policy Enforcement Point (PEP), and PDP for IdAM. Each CDC will have one or more Issuing Certificate Authorities to accommodate geographic distribution and be capable of issuing and publishing digital certificates and Certificate Revocation List(s) (CRL). PEP(s) will intercept user and resource requests and forward them to PDP(s) for adjudication. PDP(s) will relay policy access decisions back to the PEP for enforcement.

Database Security

A common database platform will be implemented at each CDC to provide a consistent approach to hardening and defending servers and the databases they support. The common platform will provide database services for each of the security zones within the CDC(s). The common database platform will include database firewall, auditing, and ABAC at the data and table levels to restrict access to critical data and monitor activity in real-time.

Storage Infrastructure

The CDC storage equipment will use a modern Storage Area Network (SAN) infrastructure that is physically and logically networked according to the security zoning described in this reference architecture. The physical storage devices within the SAN will use emergent innovations such as Self Encrypting Drives (SEDs), Solid State Drives (SSDs) where appropriate and modern SAN switching equipment. The SAN will provide Redundant Array of Inexpensive Disks (RAID) capabilities for enabling Disaster Recovery and Business Continuity (DRBC) functionality as well as maintaining a mirrored, off-site storage capability.

SAN switches afford enhanced storage networking and segregation of devices on a layer three level, discriminating one Virtual Local Area Network (VLAN) from another. This functionality preserves zoning security. SAN switches also allow for Port Mirroring or Switch Port Analyzing (SPAN) of all data inbound to the switch. The inbound data can be echoed along an outbound port for monitoring or mirroring to a remote SAN performing the DRBC function.

Resiliency

CDCs must have the ability to withstand significant planned and unplanned impacts to operations while maintaining system and data availability for DoD users throughout the globe. This reference integrates resiliency characteristics into the underlying physical and logical infrastructure to withstand significant operational degradation and “fight through” adverse cyber conditions. This resiliency approach integrates security components internal to each CDC via CDC security zones, infrastructure redundancy, and the establishment of global failover capabilities. Global failover enables any CDC to assume full operational responsibility for a CDC (or other data center type) that suffers a catastrophic disruption/outage and is unable to operate in any meaningful capacity. The four resiliency areas of focus: Power, Communications, Data and Applications.

The underlying utilities supporting any CDC must be sufficient and resilient to the point that no single interruption of power will cause a complete failure or outage at a CDC. In accordance

with the Core Data Center Reference Architecture, all CDC(s) will adhere to the electrical systems standards specified for Tier III data centers per TIA-942 facility standards.

Communications resiliency is a key component in maintaining a core data center environment. Due to the critical processing and communications needs it is a requirement that each CDC have redundant communications capabilities to the internet and other CDC(s).

Data resiliency is the availability of data to and for applications and users when the original host system fails. Application resiliency is the ability to start, stop, restart and switch the execution of applications from backup systems in the event of host system failures.

The key non-security requirements underlying resiliency are incorporated in the facility infrastructure, computing infrastructure, and capability delivery sections of this reference architecture (Sections 3.1, 3.2, and 3.3)

3.4.2 Principles and Rules

Security/IA principles and rules are found in **Error! Reference source not found..**

Table 6 - Security/IA Principles and Rules (OV6a/4)

Rule #	Rule Description	Supporting Rationale/Comments
Principle #1: Core Data Centers will conform to all DoD security/IA policies and authoritative technical guidance		
1.	CDCs shall implement the DoD DMZ policy per approved security architectures, Security Requirements Guides (SRGs) and Security Technical Implementation Guides (STIGs)	DoD NIPRNET DMZ STIG
2.	CDCs shall implement network boundary protection per the approved JIE Single Security Architecture (SSA)	JIE SSA is under development
3.	CDCs shall, at a minimum, conform to security and information assurance standards outlined in the DoD 8500 Series issuances	Including: DoDI 8510.01, DoDD 8570.01-M, DoDI 8500.2, DoDI 8410.02, DoDI 8520.02, DoDI 8520.03
4.	CDCs shall only operate under an Interim Authority to Operate (IATO) or current Authority to Operate (ATO) approved by the designated Certification Approval Authority (CAA) and in accordance with the approved C&A documentation	
5.	CDCs shall ensure that all hosted systems, regardless of hosting model utilized, are certified and accredited in compliance with DoD requirements by a designated CAA	SP800-60
6.	CDCs shall ensure that all operating system images include mandated security tools such as HBSS and anti-virus and follow the respective Operating System STIG	
7.	CDCs shall implement security measures to ensure the confidentiality, integrity and availability of all information as required by the mission assurance level for that information and the associated controls	SP800-53, SP800-122, SP800-137

UNCLASSIFIED

Rule #	Rule Description	Supporting Rationale/Comments
Principle # 2: Core Data Centers will be highly resilient through pro-active monitoring, redundancy, auditing and testing		
8.	CDCs shall support standard management information for identifying physical and virtual servers and their status	
9.	CDCs shall employ a centralized building management system capable of monitoring the subsystem monitors should be utilized; the system should capable of controlling, not just monitoring, the subsystems.	
10.	CDCs shall support standard access management, equipment isolation, environmental monitoring and visual monitoring	
11.	CDCs shall implement all approved security measures to ensure the confidentiality, integrity and availability of information	
12.	CDCs shall ensure that an effective network device control program (e.g., routers, switches, firewalls) is implemented and includes: instructions for restart and recovery procedures; restrictions on source code access, system utility access, and system documentation; protection from deletion of system and application files, and a structured process for implementation of directed solutions (e.g., IAVA).	Network device control is the responsibility of the enterprise. If this level of control is not maintained systems could allow unauthorized systems to utilize the network devices. Lack of enterprise control cannot ensure that the systems are protected.
13.	CDCs shall ensure that audit or other technical measures are in place to ensure that the network device controls are not compromised and that change controls are periodically tested.	Network device control is the responsibility of the enterprise. If this level of control is not maintained systems could allow unauthorized systems to utilize the network devices. Lack of enterprise control cannot ensure that the systems are protected.
Principle #3: Core Data Centers will implement zoning to accommodate the varying levels of security needed to protect DoD information, networks, and systems		
14.	CDCs shall implement Core, Specialized, Development & Test and Management security zone types as described in this reference architecture and follow on technical guidance	
15.	CDCs shall ensure that security support structures are isolated by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform security functions.	<p>The site is responsible for ensuring isolation is maintained for systems which are installed at the site.</p> <p>The security support structure maintains separate execution domains (e.g., address spaces) for each executing process.</p>
16.	CDCs shall only implement approved Enterprise Cross-Domain Solutions	
Principle #4: Core Data Center physical and personnel security will be commensurate with the highly sensitive nature and critical importance of the information handled and services provided		
17.	CDCs shall ensure that only authorized personnel with a need-to-know are granted physical access to computing facilities that process sensitive information or unclassified information that has not been cleared for release	Ensuring only authorized personnel are granted access to a site is the responsibility of the site. A system cannot satisfy this requirement.

UNCLASSIFIED

Rule #	Rule Description	Supporting Rationale/Comments
18.	CDCs shall ensure that only authorized personnel with appropriate clearances are granted physical access to computing facilities that process classified information	Ensuring only authorized personnel are granted access to a site is the responsibility of the site. A system cannot satisfy this requirement.
19.	CDCs shall ensure that every physical access point to facilities housing workstations that process or display sensitive information or unclassified information that has not been cleared for release is controlled during working hours and guarded or locked during non-work hours	This control is satisfied by the site and a system cannot satisfy the requirement.
20.	CDCs shall ensure that every physical access point to facilities housing workstations that process or display classified information is guarded or alarmed 24 X 7 and that intrusion alarms are monitored.	This control is satisfied by the site and a system cannot satisfy the requirement.
21.	CDCs shall ensure that two (2) forms of identification are required to gain access to the facility (e.g., ID badge, key card, cipher PIN, biometrics)	This control is satisfied by the site and a system cannot satisfy the requirement
22.	CDCs shall ensure that a facility penetration testing process is in place that includes periodic, unannounced attempts to penetrate key computing facilities	This control is satisfied by the site and a system cannot satisfy the requirement.
23.	CDCs shall ensure that procedures are implemented to ensure the proper handling and storage of information, such as end-of-day security checks, unannounced security checks, and, where appropriate, the imposition of a two-person rule within the computing facility	This control is satisfied by the site and a system cannot satisfy the requirement.
24.	CDCs shall ensure that current, signed procedures exist for controlling visitor access and maintaining a detailed log of all visitors to the computing facility	This control is satisfied by the site and a system cannot satisfy the requirement.
25.	CDCs shall ensure that hosted systems have digital IA/security policy management capabilities that define, enforce, and manage the digital security policy rules, guidelines and standards for securely exchanging data and services across security domains	
Principle #5: Core Data Centers will utilize strong authentication for persons and non-person entities and allow access to information only to those authorized		
26.	Each CDC shall implement enterprise Identification & Access Management (IdAM) capabilities that use Public Key Infrastructure/Encryption (PKI/PKE) throughout the infrastructure for person and non-person entities	
27.	Each CDC shall maintain a Local Registration Authority (LRA) to rapidly respond to equipment changes as well as administrative support of personnel (users)	
28.	CDC infrastructure shall support multiple LRAs so as to prevent any disruption in the continuity of operations due to personnel casualties or unavailability	
Principle #6: Core Data Centers will utilize secure database and storage platforms		
29.	CDCs shall implement a common database platform to provide a consistent approach to hardening and	

Rule #	Rule Description	Supporting Rationale/Comments
	defending servers and the databases they support	
30.	CDCs shall use modern SAN equipment and switches that both preserve resiliency through SAN mirroring to off-site storage using SPANing and preserving security of Data At Rest using Self Encrypting Drives (SEDs)	
31.	CDC shall implement best security practices for SANs of Zoning and LUN Masking	
32.	Each CDC will implement an Out of Band Management network that will be physically separate and isolated from the production network equipment.	

3.5 Standardized Operations & Processes

3.5.1 Overview

Core Data Centers may be operated by different organizations within DoD, but they will all conform to a set of standard business, operational, and IT Service Management (ITSM) processes. This will ensure that all Core Data Centers function as a single, logically seamless computing environment meeting all requirements for customer engagement, graceful fail over, disaster recovery, continuity of operations, service/capability delivery, and load balancing. DoD will minimize costs by keeping hardware, software and operations as consistent and standardized as possible, while also reducing the number of tools, activities and personnel needed to perform the same basic functions.

CDC business processes are those activities necessary for the effective and efficient management of the CDC. These processes include personnel management, financial management, logistics management, and customer relationship management. One key challenge for the Department will be developing a standard model for cost recovery, especially for non-mandatory services provided to Components through a Service Level Agreement. There are significant differences today in the way data centers perform cost accounting and cost recovery owing to many factors including whether the data center is funded through a working capital fund or appropriated funds. Section 3.5.2 Principles and Rules only address high-level guidance for standardized business processes. The JIE Technical Synchronization Office (JTSO) will oversee the development of detailed business processes for CDCs.

CDC operational processes are those activities necessary to ensure effective and efficient operation of the CDC as part of the larger JIE computing environment. These processes include backup, continuity of operations, disaster recovery, and archiving. These processes apply to the way CDCs interoperate (e.g. CDCs backing up other CDCs) and to the way CDCs provide these services to Installation Processing Nodes and other data center types. Section 3.5.2 Principles and Rules only address high-level guidance for standardized operational processes. The JIE Technical Synchronization Office (JTSO) will oversee the development of detailed operational processes for CDCs.

CDC ITSM processes are those activities necessary for the effective and efficient delivery of capabilities to customers in the form of IT services. IT service delivery takes different forms including client/server applications, cloud computing-based delivery (e.g. PaaS), and services based on a Service Oriented Architecture (SOA). The DoD CIO adapted the internationally recognized IT Infrastructure Library (ITIL)⁹ guidance into a set of DoD process guides. The *Defense ITIL Standard Process Guidance* documents⁹ contain IT Service Management (ITSM) process guidelines based on ITIL v3 and ISO 20000. The guidelines define specific (industry best practices) Service Management processes that each DoD organization, including Components, Military Services, Agencies and their Service Providers must use to effectively and efficiently manage the Department's IT infrastructure, including IT services that traverse the GIG. The guidance provides a foundation for Components to develop lower level processes that are more detailed and tailored to the organization's environment. An overview of Defense ITIL is provided in Figure 9. It depicts the five ITSM lifecycles (Service Operations, Service Design, Service Transition, Service Strategy, and Continual Service Improvement) and the individual process guides that make up each lifecycle. These process guides address four major Defense ITIL stakeholders:

- Service Owner – organization responsible for overall management and governance of the service
- Service Designer – organization responsible for the design and implementation of the service
- Service Provider – organization responsible for hosting and delivery of the service to authorized consumers
- Service Consumer – individual or organization that uses or is affected by the service

The CDCs primarily function as a Service Provider so not every aspect of every process will apply to the CDCs.

Section 3.5.2 Principles and Rules only address high-level guidance for standardized ITSM processes. The JIE Technical Synchronization Office (JTSO) will oversee the development of detailed ITSM processes for CDCs building off of the Defense ITIL guidance.

⁹ More information on Defense ITIL can be found at: https://www.intelink.gov/wiki/Defense_IT_Infrastructure_Library

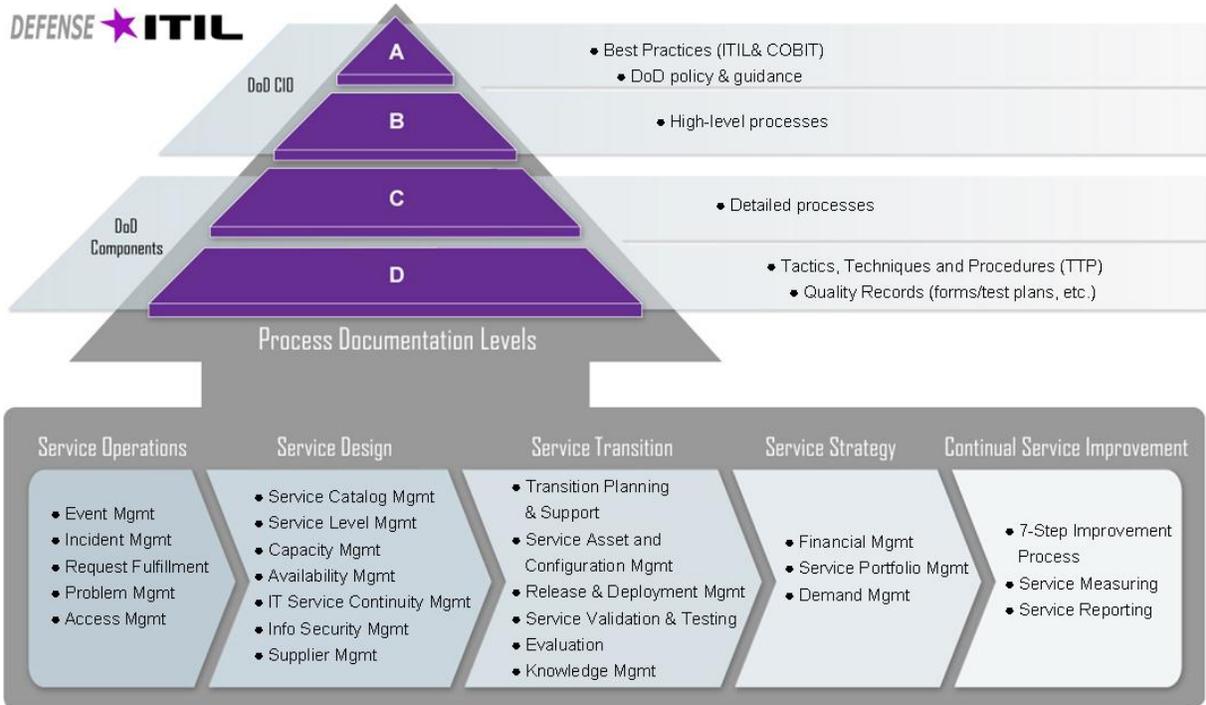


Figure 9 - Defense ITIL Overview

3.5.2 Principles and Rules

Operations and processes principles and rules are found in Table 7.

Table 7 - Operations & Processes Principles and Rules (OV-6a/5)

Rule #	Rule Description	Supporting Rationale/Comments
Principle #1: Core Data Centers will conform to standard business management processes and a “franchised” business model including personnel management, financial management, logistics/procurement management, and customer relationship management.		
1.	CDCs shall implement approved, standard processes for personnel management including training and certification of operations and maintenance personnel	Process details to be developed
2.	CDCs shall implement approved, standard processes for financial management including cost recovery associated with delivery of services per an SLA (a standard rate card)	Process details to be developed
3.	CDCs shall implement approved, standard processes for developing and managing SLAs for delivery of both Enterprise and Component-unique services	Process details to be developed
4.	CDC shall implement approved, standard processes for logistics including use of Enterprise purchasing agreements for all hardware and software procurements	Process details to be developed
5.	CDCs shall implement approved, standard	Process details to be developed

Rule #	Rule Description	Supporting Rationale/Comments
	processes for customer relationship management	
6.	CDCs shall be accredited by a third party organization per approved standards	JTSO to coordinate
Principle #2: Core Data Centers will conform to standard operational processes to ensure efficient and effective operation of the JIE computing environment.		
7.	CDCs shall ensure that monitoring processes and tools track and make available to the consumer both availability and performance metrics for critical components (servers, storage, network elements) and services	Process details to be developed
8.	CDCs shall ensure that processes and systems are in place to monitor and store (for later analysis) utilization data for: <ul style="list-style-type: none"> • CPU and memory utilization • I/O rates • Storage Utilization • Bandwidth Utilization • Device Utilization • Transaction rate • End-to-End IT service Response Time 	Process details to be developed
9.	Each CDC shall have the capability to contain, recover, restore and reconstitute during and after an incident (e.g., failure, anomaly, attack, misuse, intrusion, etc.)	Process details to be developed
10.	Each CDC shall have a detailed, documented disaster recovery and Continuity of Operations Plan (COOP) in place	Process details to be developed
11.	CDCs shall implement approved standard processes for providing backup/archive, continuity of operations, and disaster recovery services for other CDCs	Process details to be developed
12.	CDCs shall implement approved standard processes for providing backup/archive, continuity of operations, and disaster recovery services for IPNs, SPPNs, and TPNs	Process details to be developed
13.	CDCs shall exercise COOP/DR processes at least annually	
14.	CDC COOP/DR site(s) shall be at least 150 miles away and shall provide real-time, mirror backup	
15.	CDCs shall configure hosted MAC I services with an RPO of less than 1 second and an RTO of less than 30 minutes.	
16.	CDCs shall configure hosted MAC II services with an RPO and RTO of less than 8 hours	
17.	CDCs shall configure hosted MAC III services with an RPO and RTO of less than 24 hours	
Principle #3: Core Data Centers will conform to standard ITSM processes to ensure efficient and effective delivery of applications and services.		
General Rules		
18.	CDCs shall implement approved, standard ITSM processes conforming to Defense ITIL guidance or that of its successor	
19.	CDCs shall provide co-location services for	

UNCLASSIFIED

Rule #	Rule Description	Supporting Rationale/Comments
	Components	
20.	CDCs shall implement the approved, standard data vocabulary and schema designed to facilitate data sharing per the DoD Data Strategy (DoDD 8320.02)	
21.	CDCs shall ensure that configuration management data is accessible and readable by other areas within the IT Operations hierarchy including the service desk, problem management, capacity management and continuity of operations management	
Service Transition – Service Validation & Testing		
22.	CDCs shall conduct testing for all new or changed services	
23.	CDCs shall ensure that service continuity plans are tested against the service continuity requirements. Availability plans shall be tested against the availability requirements. Service continuity and availability plans shall be re-tested after major changes to the service environment in which the service provider operates.	
24.	CDC shall ensure that the results of the tests are recorded. Reviews shall be conducted after each test and after the service continuity plan has been invoked. Where deficiencies are found, the service provider shall take necessary actions and report on the actions taken.	
25.	CDCs shall ensure that all defined services are measurable, monitored and the results reported to the consumer community	
Service Transition – Incident Management		
26.	CDCs shall implement approved, standard procedures for all incidents to define: <ul style="list-style-type: none"> • Recording • Allocation of priority • Classification • Updating of records • Escalation • Resolution • Closure 	Process details to be developed
27.	CDCs shall implement the approved standard procedure for managing the fulfillment of service requests from recording to closure. Incidents and service requests shall be managed according to the procedures	Process details to be developed
28.	CDCs shall take into consideration the impact and urgency of the incident or service request when prioritizing incidents and service requests	
29.	The CDC shall ensure that personnel involved in the incident and service request management process can access and use relevant information. The relevant information shall include service request management procedures, known errors, problem	

UNCLASSIFIED

Rule #	Rule Description	Supporting Rationale/Comments
	resolutions and the CMDB. Information about the success or failure of releases and future release dates, from the release and deployment management process, shall be used by the incident and service request management process	
30.	The CDC shall keep the customer informed of the progress of their reported incident or service request. If service targets cannot be met, the CDC shall inform the customer and interested parties and escalate according to the procedure	
31.	The CDC shall document and agree with the customer on the definition of a major incident. Major incidents shall be classified and managed according to a documented procedure. Top management shall be informed of major incidents. Top management shall ensure that a designated individual responsible for managing the major incident is appointed. After the agreed service has been restored, major incidents shall be reviewed to identify opportunities for improvement	
32.	CDCs shall ensure that incident management data is visible, accessible and understandable by authorized users in accordance with the DoD Data Strategy	
33.	CDCs shall ensure that Service desk tools are present to manage incidents and changes and provide reporting capabilities	
34.	CDCs shall ensure that the Service Desk includes a ticket creation, processing, routing, tracking and reporting capability	Process details to be developed
35.	CDCs shall ensure that the Service Desk utilizes a software suite that provides the database by which the incidents are reported/opened, classified, escalated to necessary parties, monitored and resolved	Process details to be developed
Service Transition – Change Management		
36.	The CDC shall ensure that approved changes are developed and tested	
37.	CDCs shall ensure that a schedule of changes containing details of the approved changes and their proposed deployment dates are established and communicated to interested parties. The schedule of change shall be used as the basis for planning the deployment of releases	Process details to be developed
38.	CDCs shall ensure that activities required to reverse or remedy an unsuccessful change are planned and, where possible, tested	
39.	CDCs shall ensure that the change shall be reversed or remedied if unsuccessful	
40.	CDCs shall ensure that unsuccessful changes are investigated and agreed actions taken	
41.	CDCs shall ensure that the CMDB records are updated following successful deployments of	

UNCLASSIFIED

Rule #	Rule Description	Supporting Rationale/Comments
	changes	
42.	The CDC shall review changes for effectiveness and take actions agreed to with interested parties	
43.	CDCs shall ensure that requests for change are analyzed at planned intervals to detect trends	
44.	CDCs shall ensure that the results and conclusions drawn from the analysis are recorded and reviewed to identify opportunities for improvement	
45.	CDCs shall ensure that applications and application components adhere to DoD standard naming conventions, reside in common libraries and are deployed using standard release-management processes	
Service Design – Information Security Management		
46.	The CDC shall create, implement and maintain a service management plan. Planning shall take into consideration the service management policy, service requirements and requirements of the Service Management System (SMS). The service management plan shall contain or include a reference to known limitations which can impact the SMS, which includes all service management policies, objectives, plans, processes, documentation and resources required for the design, transition, delivery and improvement of services	
47.	CDC shall implement the approved, standard process for information security policy taking into consideration the service requirements, statutory and regulatory requirements and contractual obligations. Management shall: <ul style="list-style-type: none"> • Communicate the information security policy, and the importance of conforming to the policy, to appropriate personnel within the service provider, customers and suppliers. • Ensure that information security management objectives are established. • Define the approach to be taken for the management of information security risks and the criteria for accepting risks. • Ensure that information security risk assessments are conducted at planned intervals. • Ensure that internal information security audits are conducted annually. • Ensure that audit results are reviewed to identify opportunities for improvement. 	Process details to be developed
48.	CDCs shall ensure that requests for change are assessed to identify: <ul style="list-style-type: none"> • New or changed information security risks. • Potential impact on the existing information security policy and controls. 	The ISO/IEC 27000 family of standards specifies requirements and provides guidance to support the implementation and operation of an information security management system.

UNCLASSIFIED

Rule #	Rule Description	Supporting Rationale/Comments
	<ul style="list-style-type: none"> Information security incidents are managed using the incident management procedures, with a priority appropriate to the information security risks. The CDC shall analyze the types, volumes and impacts of information security incidents. Information security incidents shall be reported and reviewed to identify opportunities for improvement 	
Service Design – IT Service Continuity Management		
49.	The CDC shall implement and maintain the approved service management plan. The plan shall take into consideration the service management policy, service requirements and the SMS requirements. The service management plan shall contain or include known limitations which can impact the SMS.	
50.	CDCs shall implement the approved service continuity plan(s) which shall include at least: <ul style="list-style-type: none"> Procedures to be implemented in the event of a major loss of service, or reference to them. Availability targets when the plan is invoked. Recovery requirements. Approach for the return to normal working conditions. 	Process details to be developed
51.	CDCs shall ensure that the service continuity plan(s), contact lists and the Configuration Management Database (CMDB) are accessible when access to normal service locations is prevented	
52.	CDCs shall ensure that the availability plan(s) include availability requirements and targets	
53.	CDCs shall assess the impact of requests for change on the service continuity plan(s) and the availability plan(s)	
54.	CDCs shall ensure that availability of services are monitored, the results recorded, and compared with agreed targets. Unplanned non-availability shall be investigated and necessary actions taken	
55.	CDCs shall ensure that service continuity plans are tested against the service continuity requirements. Availability plans are tested against the availability requirements. Service continuity and availability plans are re-tested after major changes to the service environment in which the service provider operates	
56.	CDCs shall ensure the results of the tests are recorded. Reviews shall be conducted after each test and after the service continuity plan has been invoked. Where deficiencies are found, the CDC shall take necessary actions and report on the actions taken	
57.	CDCs shall implement a support plan for each	

UNCLASSIFIED

Rule #	Rule Description	Supporting Rationale/Comments
	system hosted	
Service Operations – Problem Management		
58.	Following the completion of the transition activities, the CDC shall report to interested parties on the outcomes achieved against the expected outcomes. There shall be a documented procedure to identify problems and minimize or avoid the impact of incidents and problems. The procedure for problems shall define: a) Identification; b) Recording; c) Allocation of priority; d) Classification; e) Updating of records; f) Escalation; g) Resolution; h) Closure	
59.	CDCs shall ensure that problems are managed according to the standard procedure	
60.	CDCs shall analyze data and trends on incidents and problems to identify root causes and their potential preventive action	
61.	CDCs shall ensure that problems requiring changes to a configuration item (CI) are resolved by raising a request for change	
62.	CDCs shall ensure that, where the root cause has been identified, but the problem has not been permanently resolved, the CDC identifies actions to reduce or eliminate the impact of the problem on the services. Known errors shall be recorded	
63.	CDC shall ensure that the effectiveness of problem resolution are monitored, reviewed and reported.	
64.	CDCs shall ensure that up-to-date information on known errors and problem resolutions are provided to the incident and service request management process	
Service Operations – Access Management		
65.	The CDC shall assess and document the risks to service continuity and availability of services and agree with the customer and interested parties on service continuity and availability requirements. The agreed requirements shall take into consideration applicable business plans, service requirements, service level agreements (SLAs) and risks. The agreed service continuity and availability requirements shall include at least access rights to the services	

Appendix A: Overview/Summary (AV-1)

Core Data Center Reference Architecture Version 1.0

Project Charter, Overview, and Summary Information (AV-1)

Rev: October 8, 2012

This Charter, Overview, and Summary document is an executive level presentation of the DoD Core Data Center Reference Architecture (CDC RA) development effort. In the initial phases of architecture development, it will serve as a charter to communicate key aspects of the architecture scope, context, purpose, and intent from the architecture approval authority to the architect. When the architecture effort is completed, the AV-1 will additionally provide a summary of the overall effort and include findings and recommendations.

Architecture Project Identification	
Name	DoD Core Data Center Reference Architecture
Developed By (aka "The Architect")	Office of the Deputy DoD CIO for Information Enterprise
Approval Authority	Department of Defense Chief Information Officer
Security & Access	Classification: Unclassified Document Access Level:
Architecture Status	Project Start Date: 6/13/2011 Project End Date: 09/01/2012 Approval Status: Approved Approval Date: 10/05/2012 AV-1 Registration Date: March 2012 Estimated/Actual Level of Effort: 3.0 FTE for six months/1.25 FTE for one year Estimated/Actual Costs:
Collaboration Site	https://www.intelink.gov/sites/dcscra
Assumptions and Constraints	<ul style="list-style-type: none"> ▪ CDC RA Version 1.0 will be primarily focused on Core Computing Centers. Future versions will address the broader scope of other data center types ▪ All AV-1 content reflects Version 1.0 except as otherwise stated. ▪ The CDC RA will complement and align with the data center consolidation being managed under the Federal Data Center Consolidation Initiative (FDCCI) and the ITESR/JIE effort.

Purpose and Viewpoint	
Purpose (Intended Use)	Version 1.0 of this DoD-wide reference architecture is intended to define the required characteristics (attributes) of Core DoD Data Centers in terms of the services they provide and how they provide those services. These characteristics will be established as principles, rules, standards, and patterns in the form of a DoD-wide reference architecture. This RA is intended to help enable JIE Computing Infrastructure (CI) goals for a standardized, agile, ubiquitous computing environment available to all authorized users as part of a services-based Information Enterprise (IE). This environment will provide enhanced efficiency and mission effectiveness by leveraging virtualization and cloud computing. This RA will assist Components in making data center consolidation decisions by providing a means to assess existing fixed data centers against Core Data Center criteria. An existing data center determined not to be a candidate Core Data Center should be further evaluated for potential consolidation with a core Data Center.
Questions to be Answered by the	<ul style="list-style-type: none"> ▪ How do Core Data Centers align within the JIE computing infrastructure vision? ▪ What are the required attributes of Core Data Centers in terms of facility, computing,

UNCLASSIFIED

Architecture	<p>capability delivery, security/IA, and standardized processes?</p> <ul style="list-style-type: none"> ▪ What types of services will a Core Data Center provide? ▪ What delivery models will Core Data Centers use for providing IT services? ▪ What dependencies are associated with the data center and server consolidation initiative and how does it align to other ITES&R initiatives such as Enterprise Services? ▪ What are the associated performance metrics/benchmarks for DoD Core Data Centers? (Future) ▪ What are the minimum training and certification requirements for personnel operating Core Data Centers? (Future)
Architecture Viewpoint	<p>The DoD Core Data Center Reference Architecture presents a DoD-level, end-state vision and framework for achieving Department goals for increased IT security, efficiency and effectiveness. It identifies required attributes for Core Data Centers through principles, rules, technical positions (standards), and architectural patterns.</p>

Context	
Mission	<p>This reference architecture support the ITESR/JIE vision of achieving a more secure and sustainable set of IT capabilities that are economically efficient and allow for a standardized services-based information enterprise (IE), leveraging cloud computing and providing ubiquitous computing service to authorized users at the enterprise level and the tactical edge.</p>
Goals	<p>The Core Data Center Reference Architecture has the following key goals:</p> <p>Identifying Attributes of a Core Data Center</p> <ul style="list-style-type: none"> ▪ Define the characteristics of an exemplar data center for the management of hardware, computing platforms, networks, systems management, services and applications, service desk and monitoring tools to track both user and system interfaces. ▪ Define the operations processes to include service delivery and service support processes. ▪ Ensure the security of data and information by reducing the complexity of the information environment (consolidation) and making certain that Core Data Centers operate at the minimum acceptable standards outlined within current DoD policy and technical guidance. <p>Improve Efficiency and Cost Savings</p> <ul style="list-style-type: none"> ▪ Support the reduction in costs and increase operational efficiencies associated with data centers through hardware and software consolidation, facility consolidation, and use of virtualization and cloud technologies. <p>Facilitate Implementation of Cloud Computing Capabilities</p> <ul style="list-style-type: none"> ▪ Define key facility and computing requirements needed to support future implementation in the Core Data Centers of a DoD Cloud Computing Platform. <p>Identify the Types of Services and Service Delivery Models to be Supported by Core Data Centers</p> <ul style="list-style-type: none"> ▪ Support the JIE vision that Core Data Centers will be the preferred provider of IT services for both consumers of Enterprise-wide services and Component-specific services. <p>Delivering Services to the Tactical Edge (Future)</p> <ul style="list-style-type: none"> ▪ Deliver agile access to software and applications to the tactical edge through a transition to the use of cloud services for software, data access, and storage. ▪ Provide enterprise level services through Core Data Centers enabling scalability and agility, on-demand self-service and location independent access to resources. <p>Support Server Virtualization</p> <ul style="list-style-type: none"> ▪ Operate each Core Data Center according to a set of “exemplar” computing center attributes and standards within an environment of hypervisor and hardware agnostic technology to achieve interoperability and dynamically allocate resources and multi-tenant applications (server virtualization).
Rules to be Followed/Guiding Principles	<ul style="list-style-type: none"> ▪ Conform to DoDAF v2.0 ▪ Conform to DoD Reference Architecture Description Document (June 2010) ▪ Align as a component architecture of the DoD IEA v2.0 and comply with DoD IEA v2.0 requirements for all IT architectures ▪ Align to the vision and technical direction of the ITESR/JIE ▪ Architecture content to be developed and shaped through a highly collaborative process leveraging DoD CIO, Component, and JIE subject matter experts
Linkages to Other Architectures,	Architectures, Plans, Policy and Strategy

UNCLASSIFIED

<p>Programs, Initiatives, etc.</p>	<ul style="list-style-type: none"> ▪ DoD Data Center Consolidation Plan ▪ DoD Cloud Computing Strategy ▪ Theater level Synchronization Plans (TSPs) ▪ NIST Cloud Reference Architecture ▪ Active Directory Optimization Reference Architecture (ADORA) ▪ IT Enterprise Strategy & Roadmap/JIE Vision ▪ DoD Strategic Sustainability Performance Plan ▪ DoD Electronics Stewardship Plan ▪ DoD IEA v2.0 <p>Initiatives and Programs</p> <ul style="list-style-type: none"> ▪ Base Realignment and Closure Act (BRAC) consolidation ▪ Federal Data Center Consolidation Initiative (FDCCI) ▪ Defense Information Systems Agency (DISA) Defense Enterprise Computing Center (DECC) optimization 																												
<p>Alignment to DoD IEA v2.0 Capability Taxonomy</p>	<p>The CDC RA is an extension of the DoD IEA v2.0 architectural description. It aligns primarily under the “Connect, Access and Share” and “Operate and Defend” capability areas, two of three high-level capability areas defined in the Draft DoD IEA v2.0. Mappings to individual leaf-level capabilities of the DoD IEA v2.0 that are enabled by the CDC RA are shown in the table below.</p> <table border="1" data-bbox="427 674 1336 1056"> <thead> <tr> <th>Ref #</th> <th>DoD IEA v2.0 Capability Title</th> </tr> </thead> <tbody> <tr> <td>1.1.1</td> <td>Infrastructure Provisioning</td> </tr> <tr> <td>1.1.4</td> <td>Unified Communications and Collaboration</td> </tr> <tr> <td>1.1.5</td> <td>Global Connections</td> </tr> <tr> <td>1.3.1</td> <td>Data and Functionality as Services</td> </tr> <tr> <td>2.1.1</td> <td>Continuity of Operations</td> </tr> <tr> <td>2.1.2</td> <td>IE Health and Readiness Measurement</td> </tr> <tr> <td>2.1.3</td> <td>IE Situational Awareness</td> </tr> <tr> <td>2.1.4</td> <td>Automated Configuration Changes</td> </tr> <tr> <td>2.1.5</td> <td>Dynamic Configuration Management</td> </tr> <tr> <td>2.1.7</td> <td>End-to-End Quality of Service</td> </tr> <tr> <td>2.1.9</td> <td>NetOps-Enabled Resources</td> </tr> <tr> <td>2.1.10</td> <td>New Technology Implementation</td> </tr> <tr> <td>3.3.3</td> <td>National Green IT Initiative Implementation</td> </tr> </tbody> </table>	Ref #	DoD IEA v2.0 Capability Title	1.1.1	Infrastructure Provisioning	1.1.4	Unified Communications and Collaboration	1.1.5	Global Connections	1.3.1	Data and Functionality as Services	2.1.1	Continuity of Operations	2.1.2	IE Health and Readiness Measurement	2.1.3	IE Situational Awareness	2.1.4	Automated Configuration Changes	2.1.5	Dynamic Configuration Management	2.1.7	End-to-End Quality of Service	2.1.9	NetOps-Enabled Resources	2.1.10	New Technology Implementation	3.3.3	National Green IT Initiative Implementation
Ref #	DoD IEA v2.0 Capability Title																												
1.1.1	Infrastructure Provisioning																												
1.1.4	Unified Communications and Collaboration																												
1.1.5	Global Connections																												
1.3.1	Data and Functionality as Services																												
2.1.1	Continuity of Operations																												
2.1.2	IE Health and Readiness Measurement																												
2.1.3	IE Situational Awareness																												
2.1.4	Automated Configuration Changes																												
2.1.5	Dynamic Configuration Management																												
2.1.7	End-to-End Quality of Service																												
2.1.9	NetOps-Enabled Resources																												
2.1.10	New Technology Implementation																												
3.3.3	National Green IT Initiative Implementation																												

<p>Scope: Identification of Architecture Viewpoints, Views, and non-DoDAF Products</p>	
<p>Architecture Boundaries</p>	<ul style="list-style-type: none"> ▪ The scope of Version 1.0 of the CDC RA includes an overview of the JIE Computing Infrastructure consisting of Core, Local/Installation, Special Purpose and Tactical/Mobile data centers but focuses only on characteristics of Core Data Centers. Characteristics of other types of data centers and the networks that connect them will be addressed in future versions. ▪ Version 1.0 will define the operational and support characteristics of Core Data Centers including the enterprise services to be delivered by Core Data Centers, physical facility characteristics, leveraging virtualization and cloud computing to enhance efficiency and mission effectiveness, and providing necessary steps for addressing current security vulnerabilities ▪ Version 1.0 will not address Total Cost of Ownership considerations, operational performance metrics, or enhancements that may be needed to DoD networks to fully enable cloud delivery. ▪ The objective end-state time horizon is 2017/2018
<p>DoDAF v2.0 Views Developed</p>	<p>AV-1: Overview and Scoping Document (this document) - Provides the scope, purpose, goals, intended users, environment depicted and analytical findings (if applicable)</p> <p>AV-2: Integrated Dictionary – Definition of acronyms, terms and architectural data used within the RA (Develops consistency/standardization throughout document and community)</p> <p>OV-1(s): High-level Overview Graphic – Provides an overarching view and description of the operational concept presented within the RA</p> <p>OV-5a: Operational Activity Decomposition Tree – Hierarchy of necessary operational activities to be carried out by Core DCs in the course of achieving the stated goals</p> <p>OV-6a: Operational Rules Model – High level principles and rules that are essential in achieving the goals laid out within the reference architecture. The OV-6a will cover business rules, attributes of exemplar data centers, and rules/minimal requirements for delivery of</p>

UNCLASSIFIED

	enterprise service through the Core. StdV-1: Technical Standards Profile – Table of standards that must be applied/adhered to in order to achieve the goals set forth in RA (DoDIs, DoDDs, STIGs, etc.).
Organizations Involved	DoD CIO, DISA, MilDeps, COCOMs, MHS/TMA
Security and Information Assurance Considerations	<p>Operate within standards outlined in:</p> <ul style="list-style-type: none"> o DoDD 8500.01E - Information Assurance (IA) o DoDI 8500.2 - Information Assurance (IA) Implementation o DoDI 8510.01 – DoD Information Assurance Certification & Accreditation (DIACAP) o DoDD 8570.01-M – Information Assurance Workforce Improvement Program o DoDI 8410.02 – NetOps for the Global Information Grid (GIG) o NIST SP800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems o NIST SP800-33: Underlying Technical Models for Information Technology Security o CNSSI 1253 – Confidentiality , Integrity and Availability o SP800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems o NIST SP800-30: Risk Management Guide for Information Technology Systems o NIST SP800-30 Rev. 1: DRAFT Guide for Conducting Risk Assessments o SP800-33: Underlying Technical Models for Information Technology Security o NIST SP800-34 Rev 1: Contingency Planning Guide for Federal Information Systems o NIST SP800-35: Guide to Information Technology Security Services o NIST SP800-37: Guide for Applying the Risk Management Framework to Federal Information Systems o NIST SP800-39: Managing Information Security Risk: Organization, Mission, and Information System View o NIST SP800-53 Revision 3: Recommended Security Controls for Federal Information Systems and Organizations o NIST SP800-53A Revision 1: Guide for Assessing the Security Controls in Federal Information Systems o NIST SP800-119: Guidelines for the Secure Deployment of IPv6 o NIST SP800-144: Guidelines on Security and Privacy in Public Cloud Computing o NIST SP800-145: A NIST Definition of Cloud Computing o NIST SP800-146: DRAFT Cloud Computing Synopsis and Recommendations o NSTISSP 11 - National Security Telecommunications and Information Systems Security Policy No. 11: National Information Assurance Acquisition Policy

Tools and File Formats to be Used

This architecture development effort will utilize the Microsoft Office suite of productivity applications, and other tools as needed. The project team will maintain a repository of information and data relevant to the effort. All DoDAF views (formerly referred to as products) will be developed in compliance to DoDAF v2.0 conventions.

Findings and Recommendations

To be developed following architecture completion and analysis.

Appendix B: Standards Viewpoint (StdV-1)

The following table contains a list of technical and policy standards issued by DoD or industry that are applicable to CDCs. Some of the standards listed are identified in Section 3 as requirements and are considered mandatory for the purpose of compliance with this reference architecture. The remaining listed standards are considered informational.

The table is organized and sorted by the short form Standard Identifier. The full standard title and a brief abstract are also provided for each standard. The applicability column identifies which of the five requirement areas the standard supports and in some cases other information on use of the standard.

#	Standard Identifier	Standard Title	Abstract	Applicability
1.	ANSI/TIA-942-2005 (Mandatory)	Telecommunications Infrastructure Standards for Data Centers, 2005	Provides requirements and guidelines for the design and installation of a data center or computer room. Is intended for use by designers who need a comprehensive understanding of the data center design including the facility planning, the cabling system, and the network design.	Facility Infrastructure
2.	CNSSI-1253 (Informational)	Committee on National Security Systems Instruction 1253: Security Categorization and Control Selection for National Security Systems, dated March 2012	Guidance tool for Information Systems Security Engineers, Authorizing Officials and Senior Agency Information Security Officers to select and agree upon appropriate protections for a National Security System	Security/IA This Instruction serves as a companion document to NIST SP 800-53 for all organizations within the National Security Community.
3.	DoD S-3020.45-V4 (Mandatory)	DoD Manual S-3020.45 Volume 4,	Defense Critical Infrastructure Program (DCIP): Defense Critical Asset (DCA) Nomination and Submission Process (U), March 20, 2009	Facility Infrastructure
4.	DoDD 8320.02 (Mandatory)	DoD Directive 8320.02: (2004) Data Sharing in a Net-Centric Environment	Directs the use of resources to implement data sharing among information capabilities, services, processes, and personnel interconnected within the Global Information Grid (GIG)	Operations/ Processes
5.	DoDD 8500.01E (Mandatory)	DoD Directive 8500.01: Information Assurance (IA)	Establishes policy and assigns responsibilities to achieve Department of Defense (DoD) information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and	Security/IA Applies to all DoD-owned or - controlled information systems that

UNCLASSIFIED

#	Standard Identifier	Standard Title	Abstract	Applicability
			technology, and supports the evolution to network centric warfare.	receive, process, store, display or transmit DoD information, regardless of mission assurance category, classification or sensitivity
6.	DoDD 8570.01-M (Mandatory)	DoD Directive 8570.01-M: Information Assurance Workforce Improvement Program	Provides guidance and procedures for the training, certification, and management of the DoD workforce conducting Information Assurance (IA) functions in assigned duty positions.	Security/IA
7.	DoDI 8500.2 (Mandatory)	DoD Instruction 8500.2: Information Assurance (IA) Implementation	Implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks	Security/IA
8.	DoDI 8510.01 (Mandatory)	DoD Instruction 8510.01: DoD Information Assurance (IA) Certification and Accreditation Process (DIACAP)	A process to ensure that risk management is applied on information systems (IS), defining a DoD-wide formal and standard set of activities, general tasks and a management structure process for the certification and accreditation (C&A) of a DoD IS that will maintain the information assurance (IA) posture throughout the system's life cycle	Security/IA
9.	DoDI 8410.02 (Mandatory)	DoD Instruction 8410.02: NetOps for the Global Information Grid (GIG)	Institutionalizes NetOps as an integral part of the GIG, establishes policy, and assigns responsibilities for implementing and executing NetOps, the DoD-wide operational, organizational, and technical capabilities for operating and defending the GIG.	Operations/ Processes Applies to all GIG information systems; associated processes, personnel, and technology; and GIG interfaces to DoD mission partners
10.	DoDI 8520.02 (Mandatory)	DoD Instruction 8520.02: Public Key Infrastructure (PKI) and Public Key Enabling (PKE)	Establishes and implements policy, assign responsibilities, and prescribe procedures for developing and implementing a DoD-wide PKI and enhancing the security of DoD information systems by enabling	Security/IA Applies to all unclassified and classified DoD information

UNCLASSIFIED

#	Standard Identifier	Standard Title	Abstract	Applicability
			these systems to use PKI for authentication, digital signatures, and encryption.	systems and networks and all users accessing these information systems
11.	DoDI 8520.03 (Mandatory)	DoD Instruction 8520.03: Identity Authentication for Information Systems	Implements policy in DoDD 8500.01E, assigns responsibilities, and prescribes procedures for implementing identity authentication of all entities to DoD information systems.	Security/IA Applies to all DoD unclassified and classified information systems including networks, Defense Research and Engineering Network, Secret Defense Research and Engineering Network web servers, and e-mail systems.
12.	FIPS 140-3 (Mandatory)	Federal Information Processing Standard (FIPS) Version 140-3	Revised version of the Federal Information Processing Standards Publication 140-2: Security Requirements for Cryptographic Modules. Provides a set of cryptographic modules (algorithms) – requirements that must be satisfied by a product before being considered for government acquisition.	Security/IA Operations/ Processes
13.	FIPS 199 (Informational)	Federal Information Processing Standard (FIPS) Version 199: Standards for Security Categorization of Federal Information and Information Systems	A United States Federal Government standard that establishes security categories of information systems used by the Federal Government, one component of risk assessment. FIPS 199, along with FIPS 200, are mandatory security standards as required by FISMA. FIPS 199 requires Federal agencies to assess their information systems in each of the categories of confidentiality, integrity and availability, rating each system as low, moderate or high impact in each category. The most severe rating from any category becomes	Capability Delivery Security/IA

UNCLASSIFIED

#	Standard Identifier	Standard Title	Abstract	Applicability
			the information system's overall security categorization.	
14.	ISO/IEC 20000-1:2011 (Informational)	International Organization for Standards 20000-1:2011 – IT Service Management	International standard guiding the design, transition, delivery and improvement of services that fulfill service requirements and provide value for both the customer and the service provider. Requires an integrated process approach when the service provider plans, establishes, implements, operates, monitors, review, maintains and improves a service management system.	Operations/ Processes
15.	ISO/IEC 27000 (Informational)	International Organization for Standards 27000: Information Technology Security Techniques — Information Security Management Systems — Overview and Vocabulary.	A family of related standards on Information Security Management Systems	Operations/ Processes
16.	ITU-T X.509 (Mandatory)	International Telecommunications Union, Telecommunications Standard X.509: Information technology – Open systems interconnection – The Directory: Public-key and Attribute Certificate Frameworks	In cryptography, X.509 is an ITU-T standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI). X.509 specifies, amongst other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.	Security/IA
17.	NSTISSP 11 (Informational)	National Security Telecommunications and Information Systems Security Policy No. 11: National Information Assurance Acquisition Policy	This document is a national policy factsheet applicable to the security of national security telecommunications and information systems.	Security/IA
18.	SP800-119 (Mandatory)	NIST SP800-119: Guidelines for the Secure Deployment of IPv6	Provides information security guidance to organizations that are planning to deploy IPv6 technologies or are simply seeking a better understanding of IPv6.	Computing Infrastructure Security/IA
19.	SP800-122	NIST SP800-122:	Assists Federal agencies in	Security/IA

UNCLASSIFIED

#	Standard Identifier	Standard Title	Abstract	Applicability
	(Mandatory)	Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)	protecting the confidentiality of personally identifiable information (PII) in information systems. The document explains the importance of protecting the confidentiality of PII in the context of information security and explains its relationship to privacy using the Fair Information Practices.	
20.	SP800-137 (Informational)	NIST SP800-137: Information Security	Assists organizations in the development of an ISCM strategy and the implementation of an ISCM program that provides awareness of threats and vulnerabilities, visibility into organizational assets, and the effectiveness of deployed security controls.	Security/IA
21.	SP800-14 (Mandatory)	NIST SP800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems	Offers generally accepted principles based on the premise that , unless specific circumstances apply, everyone applies these when developing or maintaining a system	Security/IA Applicable to all aspects of the DoD Data Center and Server Consolidation effort
22.	SP800-144 (Informational)	NIST SP800-144: Guidelines on Security and Privacy in Public Cloud Computing	Provides an overview of public cloud computing and the security and privacy challenges involved. Discusses the threats, technology risks, and safeguards for public cloud environments, and provides the insight needed to make informed information technology decisions on their treatment.	Computing Infrastructure Security/IA
23.	SP800-145 (Informational)	NIST SP800-145: A NIST Definition of Cloud Computing	Characterizes important aspects of cloud computing and is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing.	Computing Infrastructure
24.	SP800-146 (Informational)	NIST SP800-146: Cloud Computing Synopsis and Recommendations	Provides recommendations for IT decision makers and explains cloud computing technology in plain terms.	Computing Infrastructure
25.	SP800-30 (Informational)	NIST SP800-30: Risk Management Guide for Information Technology Systems	Provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within	Security/IA Operations/ Processes

UNCLASSIFIED

#	Standard Identifier	Standard Title	Abstract	Applicability
			IT systems.	
26.	SP800-30 Rev. 1 (Informational)	NIST SP800-30 Rev. 1: DRAFT Guide for Conducting Risk Assessments	Summarizes the HIPAA security standards and explains some of the structure and organization of the Security Rule.	Security/IA Operations/ Processes
27.	SP800-33 (Mandatory)	NIST SP800-33: Underlying Technical Models for Information Technology Security	Provides a description of the technical foundations (models) that underlie secure information technology (IT) and should be considered in the design and development of technical security capabilities. (Lessons learned best practices, and specific technical considerations)	Security/IA Operations/ Processes
28.	SP800-34 Rev 1 (Informational)	NIST SP800-34 Rev 1: Contingency Planning Guide for Federal Information Systems	Assists organizations in understanding the purpose, process, and format of information system contingency planning development through practical, real-world guidelines.	Operations/ Processes
29.	SP800-35 (Mandatory)	NIST SP800-35: Guide to Information Technology Security Services	Provides assistance with the selection, implementation, and management of IT security services by guiding organizations through the various phases of the IT security services life cycle.	Capability Delivery Security/IA
30.	SP800-37 (Mandatory)	NIST SP800-37: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach	Provides guidelines for applying the Risk Management Framework to federal information systems to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.	Security/IA
31.	SP800-39 (Informational)	NIST SP800-39: Managing Information Security Risk: Organization, Mission, and Information System View	Provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems.	Security/IA
32.	SP800-53 rev 3 (Mandatory)	NIST SP800-53 Revision 3: Recommended Security Controls for Federal Information Systems and	Provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government to meet the requirements of FIPS 200, <i>Minimum</i>	Security/IA

UNCLASSIFIED

#	Standard Identifier	Standard Title	Abstract	Applicability
		Organizations	<i>Security requirements for Federal Information and Information Systems.</i>	
33.	SP800-53A rev 1 (Mandatory)	NIST SP800-53A Revision 1: Guide for Assessing the Security Controls in Federal Information Systems	Provide guidelines for building effective security assessment plans and a comprehensive set of procedures for assessing the effectiveness of security controls employed in information systems supporting the executive agencies of the federal government.	Security/IA
34.	SP 800-60 (Mandatory)	NIST SP 800-60a: Guide for Mapping Types of Information and Information Systems to Security Categories	Addresses the FISMA direction to develop guidelines recommending the types of information and information systems to be included in each category of potential security impact.	Security/IA
35.	Tier Standard: Topology (Mandatory)	Data Center Site Infrastructure Tier Standard: Topology, 2010	Published by the Uptime Institute, LLC. Describes criteria to differentiate four classifications of site infrastructure topology based on increasing levels of redundant capacity components and distribution paths.	Facility Infrastructure
36.	UFC 4-010-01 (Mandatory)	Unified Facilities Criteria: DoD Minimum Antiterrorism Standards For Buildings, 9 Feb 2012	DoD guidance	Facility Infrastructure
37.	UFC 4-010-02 (Mandatory)	Unified Facilities Criteria: DoD Minimum Antiterrorism Standoff Distances For Buildings, 9 Feb 2012	DoD guidance	Facility Infrastructure

Appendix C: Operational Activity Node Tree (OV-5a)

The set of CDC operational activities was developed to categorize the activities and functions that a CDC must provide. The OV-5a is structured as a hierarchical, parent/child node tree with each child node providing an increased level of detail relative to its parent node. The top node, “Perform Core Data Center Operations”, is labeled “A0”. The five second level nodes (child nodes of A0) are labeled A1 through A5. The third level nodes (child nodes of A1 through A5) are labeled with the second level node designator followed by a decimal point and the number of that third level node. For example, the third level nodes of A1 would be labeled A1.1, A1.2, etc. Fourth level nodes would follow the same convention (e.g. A1.2.3).

The five second level nodes (A1 – A5) were used as the basis for corresponding sets of tables identifying the principles, rules and standards applicable for each of the five categories. In the future, the OV-5a will be used to identify and develop operational process models to guide detailed operational processes that all CDCs must follow. Definitions for the activity nodes can be found in the Integrated Dictionary in Appendix D.

Figure 10 shows the top two levels of the hierarchy. Figures 10 through 14 show the further hierarchical breakdown of each of the five second level nodes.

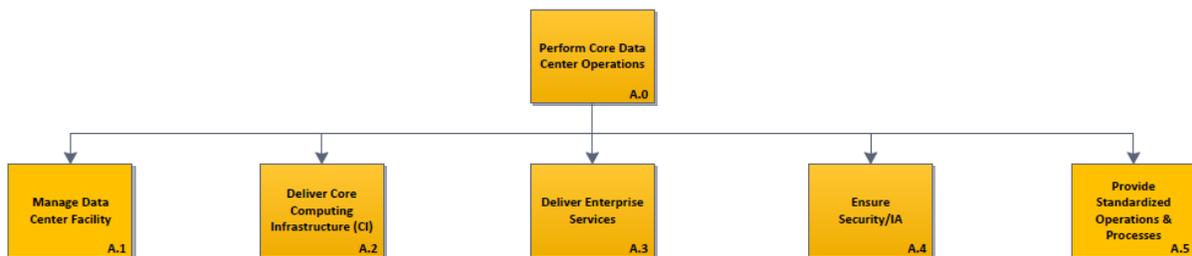


Figure 10 - Node Tree Level 0 and Level 1

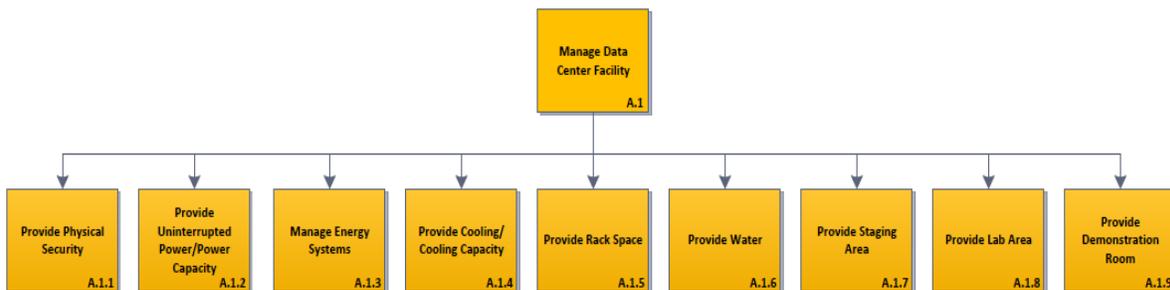


Figure 11 - Manage Facility Infrastructure Nodes

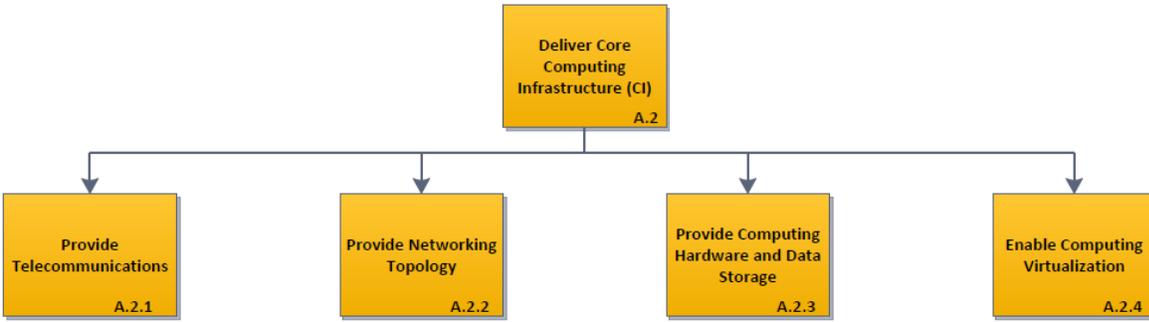


Figure 12 - Manage Computing Infrastructure Nodes

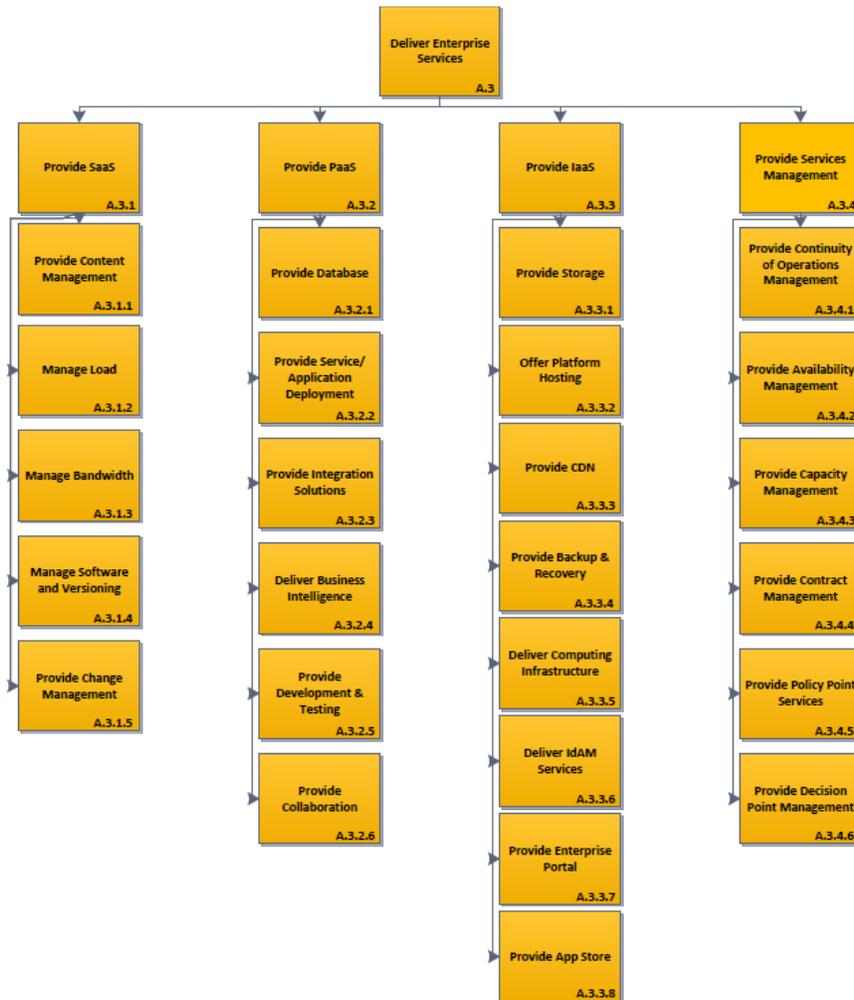


Figure 13 - Deliver Capabilities Nodes

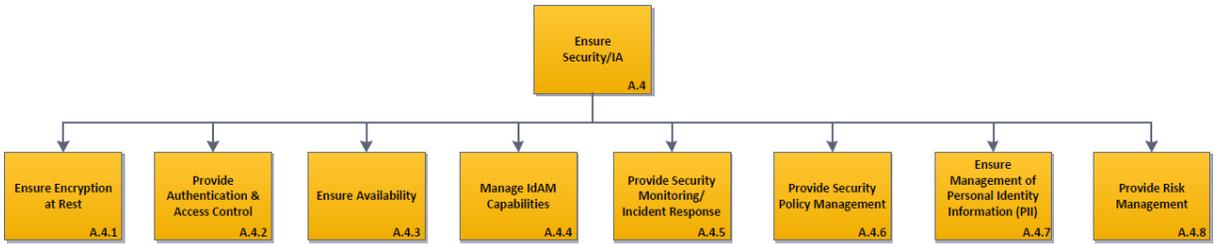
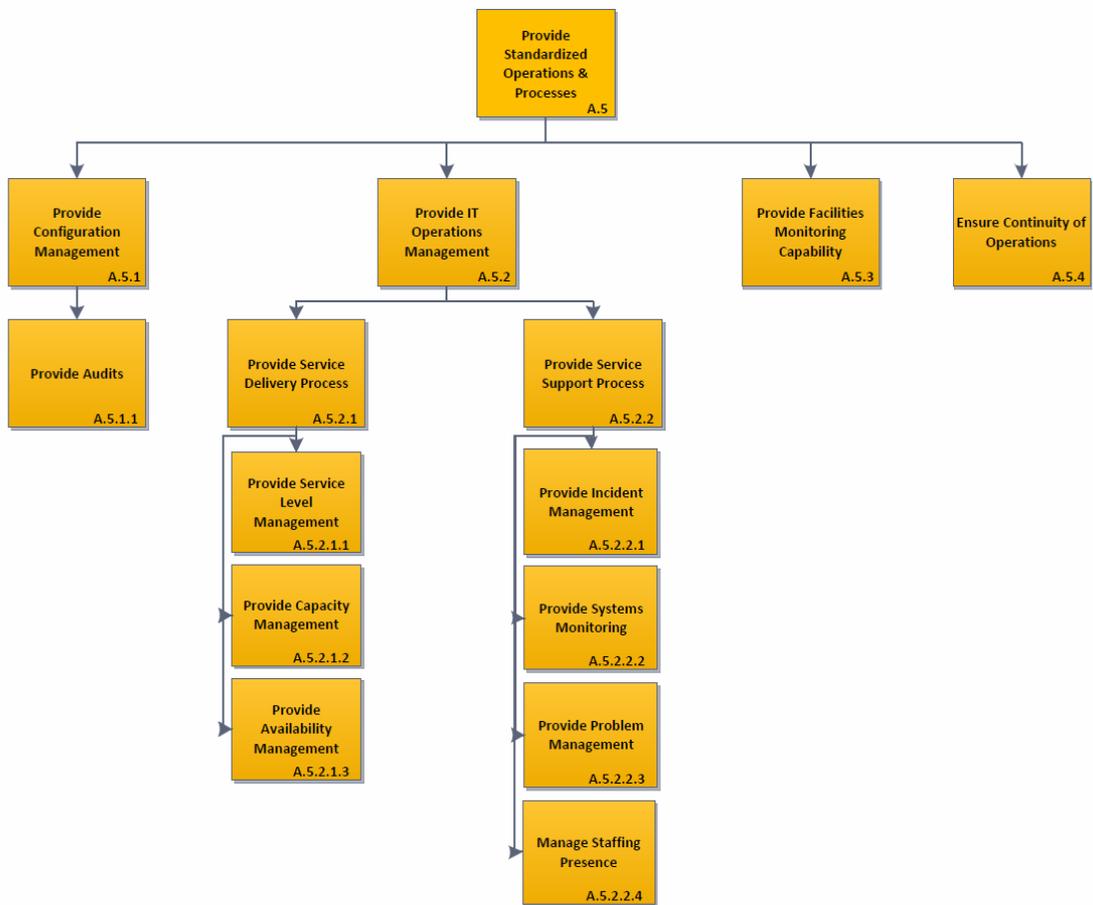


Figure 14 - Ensure Security/IA Nodes

Figure 15 - Provide Operations & Processes Nodes



d

Appendix D: Glossary and Integrated Dictionary

D.1 - Glossary

Acronym	Name
ACL	Access Control List
ABAC	Attribute Based Access Control
ADORA	Active Directory Optimization Reference Architecture
AES	Advanced Encryption Systems
AICPA	American Institute of Certified Public Accountants
ATO	Authority to Operate
AV	All View (DoDAF)
BRAC	Base Realignment and Closure Act
C&A	Certification and Accreditation
CAA	Certification Approval Authority
CDC	Core Data Center
CDP	Certificate Distribution Point
CDS	Cross-Domain Services
CI	Computing Infrastructure
CL	Confidentiality Levels
CMDB	Configuration Management Database
CNSSI	Committee on National Security Systems Instruction
CONOPS	Concept of Operations
COOP/DRP	Continuity of Operations Planning/Disaster Recovery Planning
CRL	Certificate Revocation List
C/S/A	Combatant Command/Military Service/Defense Agency
CV	Capability View (DoDAF)
DAA	Designated Accrediting Authority
DCA	Defense Critical Asset
DCIP	Defense Critical Infrastructure Program
DECC	Defense Enterprise Computing Center
DESA	Defense Enterprise Security Architecture
DIACAP	Defense Information Assurance Certification & Accreditation Process
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoD CIO	Department of Defense Chief Information Officer
DoD IEA	Department of Defense Information Enterprise Architecture
DoDAF	Department of Defense Architecture Framework
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DR	Disaster Recovery
DRBC	Disaster Recovery and Business Continuity
DMZ	Demilitarized zone
EIEMA	Enterprise Information Environment Mission Area
EOC	Enterprise Operations Center
EOOC	Enterprise Operations Oversight Committee
ES	Enterprise Services

UNCLASSIFIED

ESM	Enterprise Service Management
EUD	End-User Device
FDCCI	Federal Data Center Consolidation Initiative
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
GIG	Global Information Grid
GIG CI	Global Information Grid Computing Infrastructure
Gbps	Gigabits per second
GTG	GIG Technical Guidance
HAIZE	High Assurance Internet Protocol Encryption
HBSS	Host Based Security System
IA	Information Assurance
IaaS	Infrastructure-as-a-Service
IAP	Internet Access Point
IATO	Interim Authority to Operate
IAVA	Information Assurance Vulnerability Alert
IdAM	Identity and Access Management
IDS	Intrusion Detection System
IE	Information Enterprise
IP	Internet Protocol
IPN	Installation Processing Nodes
IPv6	Internet Protocol Version 6
ITESR	DoD Information Technology Enterprise Strategy & Roadmap
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
JIE	Joint Information Environment
JTSO	JIE Technical Synchronization Office
JWICS	Joint World-wide Intelligence Communication System
LRA	Local Registration Authority
LUN	Logical Unit Number
MAC Level	Mission Assurance Category Level
MW	Mega-watt
NetOps	Network Operations
NIC	Network Interface Card
NIPRNET	Unclassified IP-routed Network
OV	Operational View (DoDAF)
PaaS	Platform-as-a-Service
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIN	Personal Identification Number
PKE	Public Key Encryption
PKI	Public Key Infrastructure
PN	Processing Node
POM	Program Objectives Memorandum
RA	Reference Architecture
RAID	Redundant Array of Inexpensive Disks
RDBMS	Relational Data Base Management System
RDT&E	Research, Development, Testing and Evaluation
RPO	Restoration Priority Order
RTO	Ready to Operate
SaaS	Software-as-a-Service
SAN	Storage Area Network
SAS	Statement on Auditing Standards

UNCLASSIFIED

SED	Self Encrypting Drive
SIPRNET	Secret IP-routed Network
SLA	Service Level Agreement
SMS	Service Management System
SOA	Service Oriented Architecture
SPAN	Switch Port Analyzer
SPPN	Special Purpose Processing Nodes
SRG	Security Requirements Guide
SSA	Single Security Architecture
SSD	Solid State Drive
StdV	Standards View (DoDAF)
STIG	Security Technical Implementation Guide
TCO	Total Cost of Ownership
TPN	Tactical/Mobile Processing Nodes
TSP	Theatre level Synchronization Plan
TTPs	Tactics, Techniques and Procedures
VLAN	Virtual Local Area Network
VoIP	Voice over IP
WAN	Wide Area Network
XACML	eXtensible Access Control Markup Language

D.2 – Integrated Dictionary (AV-2)

Term	Definition
CCAB	DoD Cloud Computing Approval Board: DoD CIO led board involving Military Departments, US Cyber Command and NSA that serves as an extension of the FedRAM.
Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
Cloud Broker	An entity that manages the use, performance and delivery of cloud services and negotiates relationships between <i>Cloud Providers</i> and <i>Cloud Consumers</i> .
Cloud Bursting	A technique used by hybrid clouds to provide additional resources to private clouds on an as-needed basis.
Cloud Carrier	The intermediary that provides connectivity and transport of cloud services from <i>Cloud Providers</i> to <i>Cloud Consumers</i> .
Cloud Computing	A technology by which services are provided through shared resources, software, and information to computers and other devices over a network (typically the Internet).
Cloud Consumer	Person or organization that maintains a business relationship with, and uses services from, <i>Cloud Providers</i> . (Types of services: SaaS, IaaS, PaaS)
Cloud Provider	Person, organization or entity responsible for making a service available to <i>Cloud Consumers</i> .
COI	Community of Interest: A collaborative group of DoD users that must exchange information in pursuit of its shared functions, interests, missions, or business processes, and therefore must have shared vocabulary and standards for the information it exchanges.
Community Cloud	The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premises or off premises.
Component	For the purpose of this document, Component refers to a Combatant Command, Military Service, or DoD agency
Computing Center	An enterprise designed to perform complex and labor-consuming computational work using electronic computers
Core Data Center (CDC)	<p>The most robust and capable DoD Data Centers designated as the mandatory provider of all Enterprise-wide computing and storage capabilities. They are marked by the following key attributes:</p> <ul style="list-style-type: none"> Initially operated by DISA or one of the Military Departments under a “franchise” model, but in the future may also include commercially operated Core Data Centers Standardized operations, processes and governance across all Core Data Centers Fixed/permanent facilities meeting TIA-942 Tier III standards and later Tier IV standards High bandwidth connections to the DISN core backbone Hosting of Enterprise Net-Centric applications and Core Enterprise Services and Applications, regional content staging Enterprise scale computing and storage Scalable space, power, and infrastructure Meet all “exemplar” data center criteria (Found within Section 3.0 of

UNCLASSIFIED

	<p>this reference architecture) Provide co-location services for other DoD Components</p>
Data Center	<p>A facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, and environmental controls.</p>
Deliver Business Intelligence	<p>Deliver ability to perform reporting, online analytical processing, analytics, data mining, process mining, complex event processing, business performance management, benchmarking, text mining and predictive analytics through available technologies.</p>
Deliver Core Computing Infrastructure	<p>Provide hardware and software necessary to support computing, communications, data storage, and operations</p>
Deliver Computing Infrastructure	<p>Deliver an infrastructure that consists of services delivered through shared, enterprise-level, Core Data Centers that appear as a single point of access for consumers' computing needs. Consideration of Service-Level Agreements (SLAs) may be required.</p>
Deliver Enterprise Services	<p>Host and make available all designated Enterprise services and applications for all authorized user</p>
Deliver IdAM Services	<p>Provide and manage services and processes for authentication of persons and non-persons and for making authorization decisions for access to data or resources.</p>
Enable Computing Virtualization	<p>Provide the ability to host multiple logical resources on a single physical platform</p>
Ensure Availability	<p>Data continues to be available at a required level of performance in situations ranging from normal through "disastrous."</p>
Ensure Continuity of Operations	<p>Ensure that critical operations necessary to meet mission requirements continue to be provided in the face of unplanned events</p>
Ensure Encryption at Rest	<p>Ensure that DoD data stored in computer drives, tapes, etc is encrypted per DoD requirements and that only authorized users are able to access (decrypt) the data.</p>
Ensure Management of Personally Identifying Information (PII)	<p>Ensure that PII at rest or in transit is protected from unauthorized disclosure per Federal and DoD requirements.</p>
Ensure Security/IA	<p>Ensure that all required measure are taken to protect facilities, personnel and information</p>
FedRAMP	<p>Federal Risk and Authorization Management Program: Established to provide a standard approach to Assessing and Authorizing (A&A) cloud computing services and products.</p>
Fixed Data Center	<p>Data Center that cannot physically be relocated or deployed as a whole (building, hanger, etc.)</p>
GIG CI	<p>Global Information Grid Computing Infrastructure: All automated IT resources used in the secure acquisition, storage, processing, management, control, and display of data or information. A primary emphasis on DoD hardware, software operating systems, and hardware and/or software operating systems support, which are identified as, and made discoverable and accessible for, GIG operations</p>
HA	<p>High Availability: Computing platforms must general feature HA characteristics that allow system operation to continue in the event of a single component failure</p>
Hybrid Cloud	<p>The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g. cloud bursting for load balancing</p>

UNCLASSIFIED

	between clouds)
Implement IdAM	<u>Identity and Access Management</u> : Management of user authorizations, e.g., Privilege Management, Role Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Risk Adaptive Access Control (RAdAC) to support both anticipated and unanticipated users
ITESR	DoD Information Technology Enterprise Strategy & Roadmap (Oct 2011)
Joint Enterprise Cloud (JEC)	Facilities, hardware, software and operations associated with the DoD Cloud environment
Joint Enterprise Cloud Platform (JECp)	Cloud platform to be implemented in order to enable cloud service availability from Core DCs
Manage Chargebacks	Management of the process by which a data center recovers costs from customers for services delivered per a Service Level Agreement (SLA)
Manage Data Center Facility	Perform all activities necessary for the proper management of physical data center facilities including security, environmental controls, and power systems.
Manage Energy Systems	Perform all activities necessary for the proper management of electrical equipment, distribution gear and service.
Manage IdAM Capabilities	Perform all activities necessary for the proper management of identity and access management capabilities.
Manage Staffing Presence	Perform all activities necessary for the proper management of assigned staff
Offer Platform Hosting	Provide a platform for hosting computing as a service, where shared resources, software and information are provided to users via various computing devices as a utility over the DoD network
Operate Service Desk	Operate a single point of contact front line support group (Help Desk) resource between the enterprise service provider and DoD users, involving the management of incidents and service requests
Perform Core Data Center Operations	Carry out all operations of a Core Data Center necessary to meet mission requirements including service to customers, disaster response, system hosting, and data storage.
Private Cloud	The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premises or off premises.
Provide App Store	Provide the capability for authorized users to access certain applications and services as self-contained modules
Provide Application Management	Provide a management process based upon a set of best practices proposed to improve the overall quality of IT software development and support through the life-cycle of software development projects, with particular attention to gathering and defining requirements that meet DoD enterprise-level IT objectives
Provide Audits	Conduct monitoring and assessment activities necessary to meet designated performance or management measures
Provide Authentication & Access Control	Provide a way of: <ul style="list-style-type: none"> • Authenticating and authorizing users to gain access to web applications and services • Establishing the validity of a transmission, message, or originator, • Verifying an individual's authorization to receive specific categories of information.
Provide Availability Management	Manage the availability of IT services through definition, analysis, planning, measurement and improvement as the party responsible for ensuring that all IT infrastructure, processes, tools, and roles are

UNCLASSIFIED

	appropriate for established service-level targets
Provide Backup & Recovery	Provide application and service backup and recovery as one of the risk mitigation/incident management factors in assuring service continuity across the DoD enterprise
Provide Bandwidth	The ability to provide scalable transport or storage capacity as needed.
Provide Capacity Management	Provide a process for ensuring that the capacity of IT services and IT infrastructure is able to deliver established service level targets in a cost-effective and timely manner
Provide CDN	<u>Content Delivery Network</u> : Provide management of a network for the delivery of Web pages, audio, video and other Internet-based content to DoD enterprise users
Provide Change Management	Provide control of the lifecycle of all changes to enable beneficial modifications to be made with minimum disruption of enterprise-level IT services
Provide Collaboration	Provide the capability for multiple entities to effectively work together toward a common goal.
Provide Computing Hardware and Data Storage	Provide servers, storage arrays and related hardware necessary to deliver services to customers.
Provide Configuration Management	Provide a process for maintaining information about configuration items required to deliver an IT service throughout the lifecycle of the computing infrastructure, including their relationships
Provide Content Management	Provide a means of organizing and storing enterprise-level content that relates to DoD processes, including: strategies, methods, and tools used throughout the lifecycle of the content
Provide Continuity of Operations Management	Provide an operations management process that sets objectives, scope and requirements that aid in mitigating risks that could seriously impact the continuity of IT service delivery within the DoD computing infrastructure
Provide Contract Management	Carry out all activities related to the development, execution and maintenance of legally binding agreements (contracts)
Provide Cooling/Cooling Capacity	Carry out all activities to ensure that the data center facility is maintained at proper environmental levels
Provide CRM	<u>Customer Relationship Management</u> : Strategy for managing interactions with customers, clients and sales prospects involving the use of technology to organize, automate, and synchronize business processes
Provide Database	Provide the physical and logical capacity for an organized collection of data and information to support service specific processes and requirements
Provide Decision Point Management	Provide the ability to make effective decisions based on established criteria.
Provide Demonstration Room	Provide an area within the non-production portion of the data center for testing and demonstrations in support of customer needs.
Provide Development & Testing	Provide, as an aspect of continuity management, a process for the development and testing of enterprise-level services and applications to ensure conformation with security and service level requirements
Provide Document Management	Provide a system for enterprise level digital asset management, document imaging, workflow and records management
Provide Email & Office Productivity Solutions	Provide enterprise level tools/applications for e-mail and the viewing, creating and modifying of general office documents (e.g., spreadsheets, memos, presentations, letters, personal database, form generation, image editing, etc.). Office productivity tools also include applications for managing employee tasks.
Provide Enterprise Portal	Deliver a capability for the DoD Enterprise for web-based access to

UNCLASSIFIED

	Enterprise capabilities and services.
Provide Facilities Monitoring Capability	Provide activities and processes to enable the real-time monitoring of data center facility infrastructure necessary to meet mission requirements.
Provide Human Resources	Provide the function within the Department charged with the overall responsibility for implementing strategies and policies relating to the management of individuals
Provide IaaS	<u>Infrastructure-as-a-Service</u> - Definition as related to Cloud: Provide the capability for the consumer to provision processing, storage, networks, and other fundamental computing resources where they are 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).
Provide Incident Management	Provide a management process that aims to restore normal service operation (as defined within SLAs) as quickly as possible while minimizing the adverse effect on operations, ensuring that the best possible levels of service quality and availability are maintained
Provide Integration Solutions	Provide solutions for the roll-out, or deployment, of applications and services within the DoD enterprise computing infrastructure, including the design, development, test and release management
Provide IT Operations Management	Activities and processes necessary to execute the operational mission of the data center including capability delivery for customers, load balancing, archiving, data storage, and continuity of operations management.
Provide Lab Area	Provide a location within the data center for testing and corrective action on hardware and software that is separate from areas used for delivery of production services.
Provide Load Balancing	Activities and processes necessary to manage hardware, software and network capacities across multiple systems or multiple data centers.
Provide Networking Topology	Activities and processes necessary to develop and manage local and wide area networks necessary for mission requirements.
Provide PaaS	<u>Platform-as-a-Service</u> - Definition as related to Cloud: Provide the capability for the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations
Provide Physical Security	Activities and processes necessary to ensure the security and integrity of the data center facility including fences, visitor control, cameras, intrusion detection, and alarms.
Provide Policy Point Services	Automated services for the enforcement of AGBAC-based access control for authorizing user access to data center resources
Provide Problem Management	Provide a management process that aims to resolve the root causes of incidents and minimize the adverse impact of incidents and problems that are caused by errors within the IT infrastructure and prevent recurrence of incidents related to these errors
Provide Release Management	Provide a process for platform-independent and automated distribution of software and hardware, including license controls across the DoD enterprise IT infrastructure
Provide Rack Space	Provide physical space in approved equipment cabinets for hosting

UNCLASSIFIED

	customer equipment. Includes basic services such as physical security, power, and environment controls.
Provide Risk Management	Activities and processes necessary to develop a risk management plan then to use the plan to identify risks, manage risks per approved risk acceptance criteria, and mitigate the impact of adverse events.
Provide SaaS	<u>Software-as-a-Service</u> - Definition as related to Cloud: Provide the capability for the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
Provide Security Monitoring/Incident Response	Plan for monitoring network security and responding appropriately in the case of a security breach, system failure, information leak or other malicious activity that minimizes downtime and impact: <ul style="list-style-type: none"> • Identify signs of compromise or break-ins and determine the extent of the damage to your systems • Minimize the impact of the security incident • Recover systems to a fully operational state • Identify lessons learned from the security incident and make recommendations that will help prevent future reoccurrences • Provide a formal incident response plan for compliance audits
Provide Security Policy Management	Provide and manage information security protections commensurate with the risk and magnitude of the harm that may result from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems
Provide Service/Application Deployment	Activities and processes necessary to host/deploy Enterprise or Component unique services or applications in the data center.
Provide Service Delivery Process	Activities and processes necessary to deliver Enterprise or Component unique services or applications hosted in the data center.
Provide Service Level Management	Activities and processes necessary to manage the delivery of Enterprise and Component unique services or applications including the development and management of SLAs and MOAs.
Provide Services Management	Provide process-focused management for DoD enterprise IT systems focused on providing a framework to structure IT-related activities and the interactions of IT technical personnel with DoD enterprise users
Provide Service Support Process	Provide support services for ensuring that users have access to the appropriate services to support mission functions
Provide Software and Versioning	Activities and processes necessary to manage multiple versions of software including configuration management and release management.
Provide Staging Area	Provide a physical location within the data center to stage equipment and systems that are in the process of being transitioned into the production (on-line) environment.
Provide Standardized Operations & Processes	Activities necessary to develop and manage a common, standard set of processes for facility operation, technology management, and IT service management.
Provide Storage	Provide management of enterprise-level data and information storage solutions for users across the department
Provide Systems Monitoring	Activities and processes, including automated processes, for assessing the operational configuration and performance of data center systems.

UNCLASSIFIED

Provide Telecommunications	Provide hardware, software, and facility for the management of communications equipment necessary for operation of the data center.
Provide Uninterrupted Power/Power Capacity	Provide systems such as multiple commercial power feeds, backup generators, and uninterruptible power supplies to ensure the continuity of data center operations.
Provide Water	Provide water systems necessary for data center cooling or other utilities as well as potable water for the facility itself.
Public Cloud	The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
Reference Architecture (RA)	An authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions.
SLA	<u>Service Level Agreement</u> : Part of a service contract where the level of service is formally defined including references to the contracted delivery time (of the service) or performance
Tier I	<u>Basic Site Infrastructure</u> : As defined by the Uptime Institute, a Tier I basic data center has non-redundant capacity components and a single non-redundant distribution path serving the computer equipment
Tier II	<u>Redundant Site Infrastructure Capacity Components</u> : As defined by the Uptime Institute, a Tier II data center has redundant capacity components and a single, non-redundant distribution path serving the computer equipment
Tier III	<u>Concurrently Maintainable Site Infrastructure</u> : As defined by the Uptime Institute, a concurrently maintainable, Tier III, data center has redundant capacity components and multiple independent distribution paths serving the computer equipment. Only one distribution path is required to serve the computer equipment at any time. All IT equipment is dual-powered and installed properly to be compatible with the topology of the site's architecture. Transfer devices, such as point-of use switches, must be incorporated for computer equipment that does not meet this specification.
Total Cost of Ownership (TCO) Model	Model for financial estimate whose purpose is to help consumers and enterprise managers determine direct and indirect costs of a product or system. TCO is also sometimes referred to as Total Ownership Cost (TOC)