Defense Acquisition University

DoD Cloud Computing Acquisition Guidebook

November 2019

Version 1.2

This page intentionally left blank

DOCUMENT CHANGE HISTORY

Version	Date	Change
1.0	18 December 2018	Initial Version
1.1	20 April 2019	Updated with latest DoD Cloud Strategy (references, executive summary and 4.2.1) Updated Financial Audit Requirements (added paragraph 4.2.3.4) to include Special Organization Considerations (SOC) Added additional strategic contracting considerations in paragraph 4.2.5 Added paragraph (4.2.7) on using Services Contracts (DoD 5000.74) for acquiring Cloud Services
1.2	5 November 2019	Added sections 4.3.4.5 Testing and 4.4.6 Cybersecurity T&E Added additional Testing considerations in applicable areas such as in definitions, references, and Service level agreements (SLAs) Added DoD Digital Modernization Strategy to References Updated status of ISO/IEC 19086-1:2016 Standard (Information technology — Cloud computing — Service level agreement (SLA) framework — Part 1: Overview and concepts) Added (DRAFT) NIST Special Publication 800-171B Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations Enhanced Security Requirements for Critical Programs and High Value Assets Added CIO Cloud Smart Application Rationalization Playbook to references Updated references for DoD Enterprise DevSecOps Added “Reference Design Version 1.0 12 August 2019 (public)” and the DoD A&S and CIO signed memo “Software Development, Security, and Operations for Software Agility” Added Navy Cloud Broker Information and Air Force Cloud One Information to Section 6.0

ACKNOWLEDGEMENTS / LEGAL STATEMENT:

The following DoD/Federal government personnel (or FFRDC support) provided content to this Guidebook:

Author: Ardis B. Hearn, Defense Acquisition University (DAU)

CASTLE Team – Scott Stewart (DISA), Jodi Cramer (USAF) for CASTLE guide

Mr. Ashley P. Moore, MBCI, CEAP™, CPIC-P™ Director, IT Risk Management Division (T/CR) Office of the Chief Information Officer (CIO) United States Agency for Global Media (USAGM)

Kim Kendall, Cybersecurity Department, DAU

National Geospatial-Intelligence Agency NGA Cloud Team (2018)

George "Lee" Kennedy, Institute for Defense Analyses, Information Technology and Systems Division

Susan May, MITRE, Principal Cyber Security Engineer

Sarah M. Standard, Cybersecurity/Interoperability Technical Director, OUSD R&E, D-DT&E

Executive Summary

DoD agencies are struggling with how to utilize existing acquisition methods to acquire cloud services that use consumption and rate-based business models. Cloud computing presents an enormous paradigm shift from the usual acquisition model for acquiring traditional Information Technology (IT) services. An understanding of how to acquire IT "as-a-service" must be addressed in order to obtain the benefits that these services can provide. The technology is mature and available commercially and therefore a lesser concern than the existing business and contracting models. This Guidebook provides information and best practices that will allow programs to take advantage of the opportunities provided by cloud services. This new paradigm requires agencies to understand how to acquire critical services and re-think not only the way they acquire IT services in the context of deployment, but also how the IT services they consume provide mission and support functions on a shared basis. This Guidebook also includes information on the importance of understanding the commercial cloud environment as well as how solid planning can avoid potential risk areas such as vendor-lock and hidden costs.

The December 2018 DoD Cloud Strategy laid out clear objectives required to meet warfighter needs.

"DoD will continue to rely on its ability to process and disseminate information for military operations, intelligence collection, and related activities. To ensure this, the Department must address the unique mission requirements through a multi-cloud, multi-vendor strategy that incorporates a General Purpose cloud and Fit For Purpose clouds (reference Appendix A of the DoD Cloud Strategy). To this end, this strategy will design objectives around solving these strategic challenges:

• Enable Exponential Growth

• Scale for the Episodic Nature of the DoD Mission

• Proactively Address Cyber Challenges

• Enable AI and Data Transparency

• Extend Tactical Support for the Warfighter at the Edge

• Take Advantage of Resiliency in the Cloud

• Drive IT Reform at DoD "

The DoD Digital Modernization Strategy signed in July 2019 also laid out the DoD CIO vision which includes four top priorities: Cybersecurity; Artificial Intelligence (AI); Cloud; and Command, Control and Communications (C3)

(See Appendix F of this Cloud Guidebook for the full references.)

This Guidebook will aid in implementing this strategy by providing a broad overview of Cloud computing terminology and concepts in addition to detailed considerations for DoD Personnel based on their roles and responsibilities in the acquisition of IT capabilities.

The Guidebook is aligned with DoD Instruction (DoDI) 5000.02, DoDI 5000.74, DoDI 5000.75, the Defense Acquisition University's (DAU) Introduction to Cloud Computing (CLE 075), and the Defense Acquisition Guidebook (DAG). Other key references include:

15 December 2014 DoD CIO memo regarding *Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services defines*

The Federal and Department of Defense (DoD) *Cloud Computing Strategies*

The DoD Joint Information Environment (JIE)

The DoD Chief Information Officer's *DoD Cloud Way Forward*

1. NIST Guidelines on Security and Privacy in Public Cloud Computing
2. The DoD Cloud Computing (CC) Security Requirements Guide (SRG)
3. 7. Financial Statement Audit Requirements for Service Organizations (DoD Cloud Way Forward)
4.
5. 8. DOD Cybersecurity T&E Guidebook v2, Change 1 April 2018; Addendum: Cybersecurity T&E of DoD Systems
6. Hosted on Commercial Cloud Service Offerings. (https://www.dau.edu/cop/test/Pages/Documents.aspx)

For a full list of references, refer to Appendix F: References.

This page intentionally left blank

Table of Contents

List of Figures

List of Tables

1 Overview

1.1 Audience

With this Guidebook, executive sponsors, program managers (PMs), contracting officers (COs) and their staffs can clearly understand and be confident about their cloud acquisitions and associated deployments. The Guidebook has chapters designed to provide specific and tailored information for PMs, Contracting personnel, Engineers/IT Technical personnel, Financial Managers, Attorneys, and Cybersecurity personnel. Those individuals familiar with cloud concepts can go to the area of the Guidebook that outlines considerations that apply directly to their area of responsibility.

1.2 Applicability

The best practices information provided applies to all DoD acquisition programs and systems that have applicable requirements (e.g., defense business systems (DBS), national security systems, weapon systems, non-developmental items) regardless of their acquisition category (i.e., ACAT I, IA, II, III, IV) or their phase of the acquisition life cycle. Programs not required to follow DoDI 5000 series guidance will also benefit from following this Guidebook. The following provides definitions for basic cloud terminology. For a complete Glossary of terms used in this Guidebook, reference Appendix D.

1.3 Basic Terminology

Table 1. Definition of Basic Terms

Term	Definition
Application	Within the context of cloud computing, the term application may refer to either a cloud-enabled software offering as a service, web or mobile application (e.g. Facebook), or an application that exists on a virtual machine (e.g., Linux application). It is therefore preferable to clarify that type of application when using the term to avoid confusion. (NIST). The DoD CIO's definition may be more applicable for application owners looking to migrate to a cloud environment: An (IT) application is a conglomerate of "components" that provide or support a business function. To perform this business function an application is defined to consist of the architectural set of items (components) that are needed to provide this business function.
Application Rationalization	The reorganizing of an application portfolio to streamline the portfolio, by replacing, retiring, modernizing or consolidating applications, in accordance with a desired business outcome. (See Appendix F References for CIO's Cloud Smart Application Rationalization Playbook)

Table 1. Definition of Basic Terms

Term	Definition
As a Service (aaS)	The term “as a [cloud] Service” is a suffix describing a computing capability that supports all five essential characteristics of cloud computing.
Authorizing Official	The individual or entity responsible for accepting the risks associated within a given area of responsibility.
Big Data	An umbrella term referring both to the methods surrounding the use of very large data collections, and the characterization of efforts having a high degree of data volume, velocity, and variety. Reference Appendix G, Cloud Data Guidance for Cloud specific considerations.
Capital Expenditure (CAPEX)	The cost to buy fixed assets or to add to the value of an existing fixed asset with a useful life extending beyond the current year.
Cloud Access Point (CAP)	A DoD system of network boundary protections and monitoring devices through which cloud services outside the DoD network security boundary must traverse to connect to resources inside the DoD network security boundary.
Cloud Bursting	An application deployment model in which an application runs in a private cloud or data center and bursts into a public cloud when the demand for computing capacity spikes.
Cloud Computing	Cloud computing is the delivery of computing services—via servers, storage, databases, networking, software, analytics, and more—over the Internet (“the cloud”). It is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Cloud First	The policy announced in December 2010 by the U.S. CIO to accelerate adoption of cloud computing across the Federal government by directing agencies “to evaluate safe, secure cloud computing options before making new investments” in information technology.

Table 1. Definition of Basic Terms

Term	Definition
Cloud Security Requirements Guide (SRG)	The DoD document that provides the security requirements and guidance for cloud services; establishes the basis for granting DoD provisional authorizations; and provides guidance to DoD mission owners regarding the use of cloud services
Cloud Service Customer (CSC)	Cloud Service Customer. Sometimes referred to as the customer or the cloud consumer.
Cloud Service Providers (CSPs)	A service provider that owns, maintains and enhances its services, and houses those service elements in a location that it owns or manages. Companies offering computing services over the internet typically charge for cloud computing services based on usage, similar to how consumers are billed for water, cell phone plans, cable TV plans or electricity.
Cloud Service Offerings (CSOs)	The range or types of services offered by a CSP. A single CSP may have many CSOs.
Cloud Enabled	A software application or workload that is both ready to be hosted in an infrastructure-based cloud environment and has some capability to leverage the cloud characteristic of rapid elasticity. The expectation is only a minimal amount of configuration effort would be required to deploy (or re-deploy) the application in the cloud.
Cloud Infrastructure	The collection of hardware and software that enables the characteristics of cloud computing. The consumer of a cloud service does not manage or control the underlying cloud infrastructure. Cloud Infrastructure is represented in SP 500-292 NIST Cloud Computing Reference Architecture (CCRA) within the 'Resource Abstraction and Control' layer and Hardware layer.
Cloud Smart	New Federal government cloud strategy. The policy looks to build on Cloud First by ensuring the technology fits the mission that you're trying to serve. While the 2010 Cloud First policy asserted the potential benefits of cloud, Cloud Smart will stress mission outcomes. The Cloud Smart policy establishes workforce, procurement and security as the main pillars of the strategy, three areas often linked together when talking about current IT modernization.

Table 1. Definition of Basic Terms

Term	Definition
Computer Network Defense (CND)	The defense and protection of networks and information systems, detection of threats, and response to incidents.
Containerization	Containerization is an OS-level virtualization to deploy and run distributed applications without launching a separate virtual machine for each application. It is an alternate method to virtualization for cloud architectures.
Fit-for-Purpose (F2P) Cloud	DoD's definition for F2P is a cloud environment that meets highly specialized mission requirements that cannot easily be met through a General Purpose Cloud solution and is suitable for scaling to adopt new DoD customers at the enterprise level. Determination criteria include utility for mission, ease of management (including provisioning and reporting), and contract terms.
General Purpose Cloud (GPC)	DoD defines GPC as Infrastructure and Platform as a Service offerings that meet the majority of the DoD's cloud computing needs across all Components of the enterprise organization.
Hypervisor	A hypervisor is software, firmware or hardware that allows multiple operating systems to share a single hardware host. Each operating system appears to have the host's processor, memory, and other resources all to itself. Each virtual representation is called a virtual machine. The physical hardware on which a hypervisor is running is called the host machine; each virtual machine is called a guest machine.
Internal Cloud	DoD's definition of an internal Cloud is specific F2P solutions for systems and applications that need to operate in a private, on-premises cloud environment due to security or operational reasons.
Mission Owners	DoD Components and sub-components that use CSOs, i.e., The "cloud customer" or CSP's customer. Not necessarily the end user of what is in the cloud.
Multi-tenancy	A design principle allowing a single instance of a computing resource to provide separate environments to serve multiple client organizations. Each environment is virtually separated from each other and cannot view information outside of their own virtual network.

Table 1. Definition of Basic Terms

Term	Definition
Operational Expenditure (OPEX)	The ongoing cost for running a product, business, or system.
Off-Premises (DoD)	A facility (building/container) or IT infrastructure is Off-Premises if it is NOT physically or virtually on DoD owned or controlled property (i.e., On-Premises).
On-Premises (DoD)	A facility (building/container) or IT infrastructure is On-Premises if it is physically on DoD owned or controlled property. That is, it is within the protected perimeter (walls or “fence line”) of a DoD installation (i.e., Base, Camp, Post, or Station (B/C/P/S) or leased commercial space) which is under the direct control of DoD personnel and DoD security policies.
OpenDataStore	The OpenDataStore represents an architectural evolution. In the past, data belonged to and was stored and managed by applications often in semi-private data structures. In the future, data will be managed by enterprise data services and maintained in common areas accessible to all authorized users, even if the user and use is unanticipated. For an example of a cloud strategy using data, reference Appendix G, Cloud Data Guidance.
Personally Identifiable Information (PII)	The term PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. To determine whether information is PII, the agency shall perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available - in any medium or from any source - that would make it possible to identify an individual.
Physical Separation	Isolation of resources is provided by hardware controls or tangible means (e.g., an “air gap”). Note: used more with regard to separation of infrastructure within a facility.
Rationalization	The process of determining if an application should be refactored and migrated to a new platform, left on its legacy platform as-is, or sunset.

Table 1. Definition of Basic Terms

Term	Definition
Service Level Agreement	A *section* of a Cloud Computing agreement that defines the service and service levels being provided and sets performance characteristics.
Site Reliability Engineering (SRE)	The instantiation of automated System Administration functions within the cloud. Site Reliability Engineering is a discipline that incorporates aspects of software engineering and applies them to IT operations problems. The main goals are to create ultra-scalable and highly reliable software systems
Subscription Model	A business or pricing construct under which a customer must pay for access to a product or service; typically for a specific period of time (e.g., monthly, quarterly, annually).
Virtualization	The means of separating the execution of software from the underlying hardware. Virtualization is a means to provide a software representation of a physical device such as a server, storage device, or network as if it were a real single logical resource.
Virtual Machine	Software emulating a physical machine.
Virtual Separation	Isolation of resources provided by software controls (as opposed to physical means).

2 Foundations of Cloud Computing

2.1 Background

The Federal government spends over $80 billion or 31 percent of its annual IT budget on redundant and inefficient infrastructure[1]. For example, since 1998 the Federal government has increased the number of its data centers, from 432 to 2,094, a 385 percent increase. This is the opposite of what the private sector is doing. Leading companies are standardizing and centralizing these services, saving billions of dollars. Cloud computing has the potential to save billions of dollars and increase speed to market, compared to the alternative of expanding dedicated agency-specific systems implementations[2].

Still, a significant portion of Federal government spending goes towards maintaining aging and duplicative infrastructure. Instead of highly efficient IT assets enabling agencies to deliver mission services, much of this spending is characterized by low asset utilization, long lead times to acquire new services, and fragmented demand.

For instance, the 2012 NDAA Section 2867. Data Servers and Centers defines the requirement for "Migration of Defense data and government-provided services from Department-owned and operated data centers to cloud computing services generally available within the private sector that provide a better capability at a lower cost with the same or greater degree of security."

Also, on August 1, 2016, the Office of Management and Budget (OMB) issued Memorandum M-16-19, the Data Center Optimization Initiative (DCOI), which supersedes the Federal Data Center Consolidation Initiative (FDCCI) and fulfills the data center requirements of the Federal Information Technology Acquisition Reform Act (FITARA).

The DCOI requires agencies to:

- Develop and report on their data center strategies;
- Transition to more efficient infrastructure, such as cloud services and inter-agency shared services;
- Leverage technology advancements to optimize infrastructure; and
- Provide quality services for the public good.

The OMB dashboard data as of 1 May 2018 shows that the DoD has closed 202/917 or 22% of non-tiered data centers and 79/223 or 35.4% of tiered data centers[2]. The Tiered category is intended to categorize facilities that one might typically associate with the term "data center" -- a facility filled with racks of servers. The Non-Tiered category includes inefficient spaces that might contain one or only a few servers.

Cloud computing has the potential to play a major part in addressing the inefficiencies that led to the federal DCOI strategy. If managed correctly, implementing a cloud-computing model can significantly help agencies provide highly reliable, innovative services quickly despite resource constraints[3].

---

[1] https://myit-2016.itdashboard.gov/

[2] https://www.itdashboard.gov/drupal/dcoi-closures

[3] CIO Council, Creating Effective Cloud Computing Contracts for the Federal Government, Feb 24, 2012 Federal agencies must (1)

2.2 DoD Definition of Cloud Computing

The term “cloud” can create uncertainty or confusion, particularly to those lacking significant experience and education in this area. Some areas of uncertainty include how to apply contract types to meet cloud goals, how the market is structured, unfamiliarity with cloud models, and disconnects between cloud requirements and existing agency policies. These factors create the perception of barriers and slow the adoption of cloud.

This Guidebook defines and uses the term “cloud computing” as defined by National Institute of Standards and Technology (*NIST) SP 800-145, The NIST Definition of Cloud Computing:*[4]

Figure 1. Cloud Computing

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics and defines three service models and four deployment models.

This section provides a brief overview of the concepts of Cloud Computing. Specific technical considerations for each of the characteristics, service models and deployment models are found in Section 4.3 Technical Considerations (Engineers/IT Specialists).

2.2.1 Essential Characteristics

implement cloud-based solutions whenever a secure, reliable, and cost-effective cloud option exists; and (2) begin reevaluating and modifying their individual IT budget strategies to include cloud computing.

[4] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdfhttp://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Table 2. Definition of Essential Characteristics

Characteristic	Definition
On-demand self-service	Users are able to provision cloud computing resources without requiring human interaction, mostly done through a web-based self-service portal (management console).
Broad network access	Cloud computing resources are accessible over the network, supporting heterogeneous (i.e. dissimilar) client platforms such as mobile devices and workstations.
Resource Pooling	Service multiple customers from the same physical resources, by securing separating the resources on logical level (virtual separation).
Rapid Elasticity	Resources are provisioned and released on-demand and/or automated based on triggers or parameters. This will make sure your application will have exactly the capacity it needs at any point of time.
Measured Service	Resource usage are monitored, measured and reported (billed) transparently based on utilization. In short, pay for use.

2.2.2 Service Models

To be considered “cloud” the Cloud Service Models must be deployed on top of cloud infrastructure that has the key characteristics**.** Though industry sells other services such as Monitoring as a Service, Database as a Service, etc., these are the DoD Services definitions.

Table 3. Cloud Service Model Types

(See Section 4.1.2 Best Practices for PMs Acquiring Cloud for specific steps)

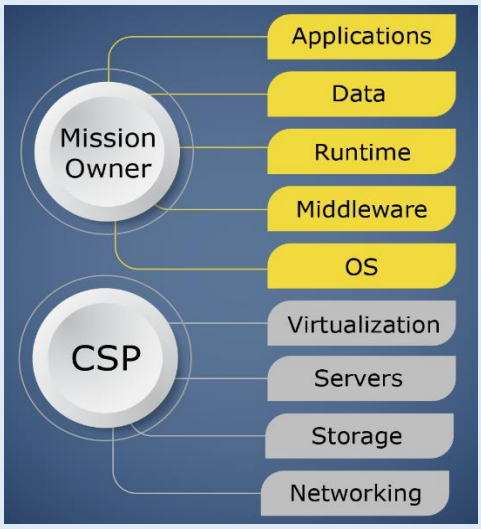
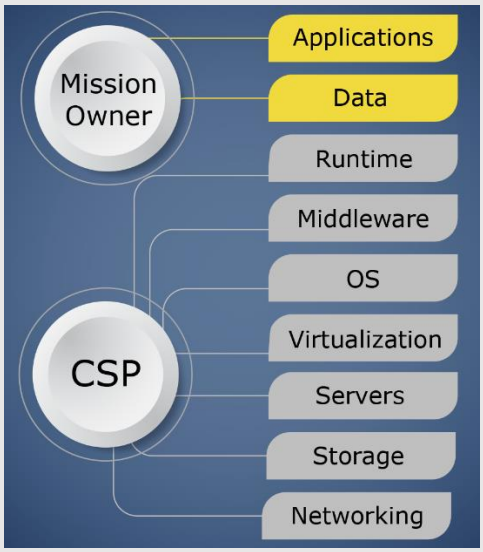
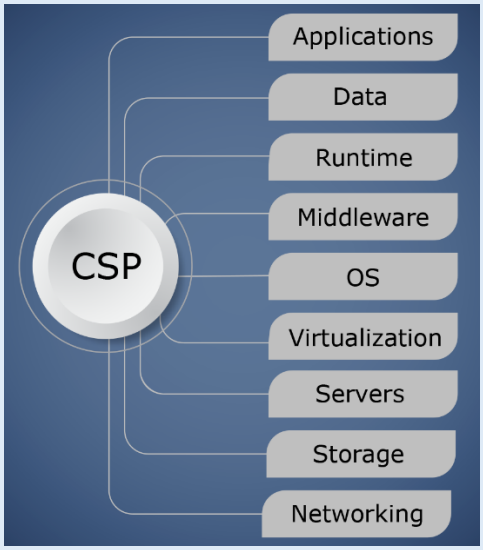
Service Model	Definition	Division of Responsibilities
Infrastructure as a Service (IaaS)	Acquire compute, storage, and networking capability. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).	
Platform as a Service (PaaS)	Deploy customer-created applications to an acquired commercial cloud infrastructure 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 configuration settings for the application-hosting environment.	

Table 3. Cloud Service Model Types

(See Section 4.1.2 Best Practices for PMs Acquiring Cloud for specific steps)

Service Model	Definition	Division of Responsibilities
Software as a Service (SaaS)	Acquire a provider's applications over a network. The consumer is responsible for managing the risk to, the quality of, and management of its data within the application. 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 and access & management of data.	

2.2.3 Four Cloud Deployment Models

Cloud computing services provide several deployment models, each of which provides distinct trade-offs for agencies that are migrating applications to a cloud environment. NIST defines the cloud deployment models as follows:

Table 4. Definition of Cloud Deployment Models

Cloud Model	Definition
Private Cloud	The cloud infrastructure is operated solely for an organization (Single Tenant). It may be managed by the organization or a third party and may exist on premise or off premise. The organization can leverage the scalability and performance aspects of cloud computing, but the infrastructure is isolated from that of other organizations, improving security and privacy. Because of their specialized nature, private clouds could potentially be as costly as dedicated data centers. For example, the DoD has a Private Cloud, milCloud, which is operated by DISA.

Table 4. Definition of Cloud Deployment Models

Cloud Model	Definition
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 premise or off premise. (On-Premise means physically located on a DoD installation). Amazon GovCloud is an example of a Community Cloud that is available to Federal, State and Local Governments.
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. Security and privacy concerns are heightened because any individual or organization can potentially access the same cloud infrastructure. Only DoD information that has been approved for public release should be placed in a public cloud.
Hybrid Cloud	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 between clouds). This model will be the most prevalent model for the DoD given its strategy to aggressively pursue the competitive acquisition and use of commercial cloud service offerings and understanding that “one cloud’ will not meet all the unique requirements of the DoD. One example of Hybrid Cloud is used in the Development – Test – Production software lifecycle.

3 DoD Approach for Acquisition of Commercial Cloud Services

Acquiring cloud services should follow normal acquisition processes with associated systems engineering rigor. In other words, acquiring cloud products and services does not mean throwing out all existing processes and practices. This means that solid requirements definition, robust market research and other *applicable* actions should take place. However, there is a difference in how to effectively harness commercial best practices in the cloud such as rate-based/consumption-based services using existing acquisition constraints. To help in these efforts, the following table provides suggested activities that specifically assist in acquiring cloud services. In addition to the information below, Appendix C in this Guidebook provides detailed Examples of different Commercial Cloud Acquisition Scenarios as an effective aid in understanding common cloud computing requirements and walks through defining an acquisition approach and understanding associated considerations.

3.1 Assessment of "As-Is" State

In order to acquire cloud services, the organization must assess, collect, list and document their "as-is" state. This will greatly enhance the organization's ability to communicate critical information to the cloud provider during the acquisition process. These are suggested steps and activities but are not all-inclusive.

Table 5. Suggested Steps and Activities Needed to Assess As-Is State

Process Steps	Activities
1. Inventory current IT Assets	• List servers (including VMs) and their OS plus any middleware components • List facilities where infrastructure is housed • List data connections for each infrastructure grouping and their capacity • List application interfaces and all dependent systems
2. Inventory and Assess current Applications and Data	• List names of stakeholders for each application, including owners, system administrators and end users • Document current physical location of host and bandwidth availability • List OS, Storage, processing, database, libraries requirements • Document Network bandwidth requirements for each application, including connection type (e.g., VPN) • Ensure there is an ATO for each application covering FISMA / FIPS PUB 199 impact level and security needs and access controls and dependencies (e.g., Microsoft Active Directory, Method of Authentication & SSO) • Define the Life expectancy of the application • Identify the number of staff and skill set needed to maintain the application (admins, programmers.) • Document the points of integration between the application and other systems. • Define Email services, such as Simple Mail Transfer Protocol (SMTP) servers for receiving outbound emails generated by the application • List Network and systems monitoring tools used by your agency's Network

Table 5. Suggested Steps and Activities Needed to Assess As-Is State

Process Steps	Activities
	Operations Center • List messaging queues such as an Enterprise Service Bus (ESBs) or other middleware • Understand what other applications depend on data furnished by the application being migrated • Create a data governance plan. A sound plan includes assessing which data is fit for the cloud. • Analyze applications that will be moved into the cloud to determine if any need to be refactored, modernized, and/or certified to run in a cloud. • Assess the application's current security posture; has the system undergone recent security testing and what are the results, could moving to the cloud improve application security or make it worse? NOTE: There is no one size that fits all solutions. Remember that not all applications should be moved to the Cloud. For example, if an application would have to be completely re-engineered to make it cloud ready, the costs to modernize the application are too significant to be beneficial. Also, an application may not meet (or may never meet) DoD security policy or security standards for on or off premise cloud environments. An application could have too many dependencies on other systems and/or interfaces or an application may be hardware dependent for failovers and redundancy.
3. Inventory Current Software Licensing	• Ensure your organization has a software manager Per OMB M-16-12 that is responsible for managing, through policy and procedure, all agency-wide commercial and COTS software agreements and licenses. Ensure you understand the details regarding licenses and software origin. Some CSPs write their agreements where they require a license per vCPU. Oracle is an example of this type of agreement. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-02.pdf • List Software licensing model (e.g., seats, servers, clients) for all applications, including cost and length of term.
4. Document Current Network	• Ensure network architecture is documented and understood, especially connection points and boundary management. • Determine whether there is sufficient connectivity, bandwidth and redundancy to support cloud services. An organization may have to make network upgrades to acquire commercial cloud services.
5. Define IT Governance	• Ensure current configuration management policies covering how current compute resources are provisioned and allocated across the departments of your agency are documented.

Table 5. Suggested Steps and Activities Needed to Assess As-Is State

Process Steps	Activities
6. Consider Agency specific Legal/ Compliance Requirements	• Ensure the PMO has the ability to maintain data per the records schedules and the ability to search and hold IAW FOIA and E-discovery.
7. Plan for Change Management[5]	• Establish a change management strategy to successfully migrate to the cloud and identify the staff needed for implementation. If the organization has solid IT Service Management (ITSM) processes in place for Asset Management, Configuration Management, and Change Management, then this activity will be much easier to manage. If not, reference the DoD Enterprise Service Management (DESMF) policy and guidance for best practices.
8. Accomplish Workforce Planning	As agencies adopt cloud platforms and related technologies, they should ensure that their staff has the skills necessary to transition to working in the cloud environment. Specifically, as part of their cloud readiness strategy, agencies should: 1. Identify their cloud skill needs beyond cybersecurity considerations; and 2. Demonstrate how they will retain, recruit, and reskill staff with these necessary skills

3.2 DoD Specific Requirements to Acquire Cloud

Once an organization accomplishes the analysis of their "as-is" state, the organization must understand the specific DoD requirements that impact their ability to acquire cloud services in the "to-be" cloud environment. The following activities are DoD specific requirements.

3.2.1 The DoD Chief Information Officer's Memo from December 2014

This memo, Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services[6], identified 5 activities when acquiring cloud services that need to be accomplished:

[5] General Services Administration (GSA), Cloud Readiness, Preparing Your Agency for Migration – Data Center Optimization Initiative (DCOI), April, 2018.

[6] DoD CIO Memo, Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services, December 2014, http://www.esi.mil/contentview.aspx?id=585

3.2.1.1 Activity 1: Perform an IT Business Case Analysis (BCA)

Each use of cloud services must be analyzed using the Enterprise IT BCA template that is explained in an earlier DoD memo: Use of Enterprise IT Standard Business Case Analysis.[7]

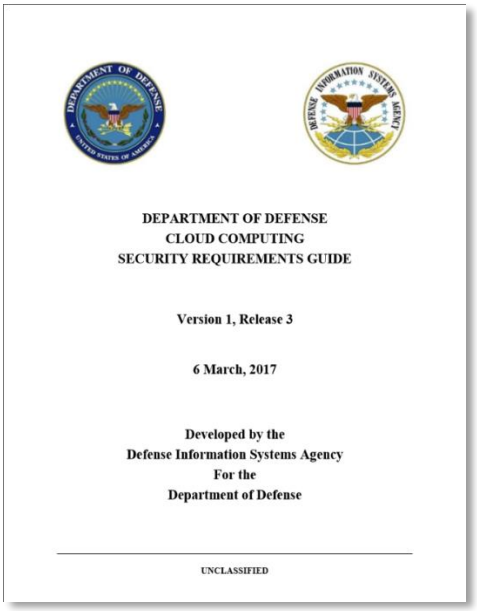
Overall Comparison of Alternatives	Financial							Non-Financial			Best Option
	NPV	Break Even	BCR	ROI	Cost (FY15-21) $M	Unfunded (FY15-21) $M	Savings (FY15-21) $M	Requirements (Exceeds, Meets, Not Acceptable)	Operational Benefits (Significant, Moderate, Low, None)	Managed Risk (Low, Med, High,	
Alternative 1 (As-Is)	N/A	N/A	N/A	N/A		N/A	N/A				←
Alternative 2											
Alternative 3											

Figure 2. IT Business Case Analysis

- Keep in mind that a BCA is not a requirements validation process. The purposes of the BCA are as follows:
  - Ensure a consistent approach in IT investment analysis.
  - Facilitate comparison of alternatives.
  - Clearly define expected costs, benefits, operational impacts, and risk.
- The major components of a BCA are:
  - Cost and economic viability
  - Requirement satisfaction/ completeness
  - Operational benefit (qualitative)
  - Risk assessment
  - Conclusions and recommendations
  - Balance cost effectiveness with operational benefit
  - Funding type and sources
- Each use of cloud services must complete an Enterprise IT Business Case Analysis (BCA)
- The BCA must be approved by the Component CIO, or designee, with a copy submitted to the DoD CIO
- Follow Component direction on completing the BCA
- DISA provided services must be considered as an Alternative in the BCA

3.2.1.2 Activity 2: Apply the DoD Cloud Computing Security Requirements Guide (SRG)

[7] DoD CIO Memo, Use of Enterprise Information Technology Standard Business Case Analysis, October 23, 2014: http://www.esi.mil/contentview.aspx?id=586.



DEPARTMENT OF DEFENSE
CLOUD COMPUTING
SECURITY REQUIREMENTS GUIDE

Version 1, Release 3

6 March, 2017

Developed by the
Defense Information Systems Agency
For the
Department of Defense

UNCLASSIFIED

Figure 3. Security Requirements Guide (SRG)

Understanding the SRG[8] is crucial in acquiring cloud services. Commercial companies and Government cloud providers are authorized to provide cloud offerings for different levels of data. The definitions for these data levels are laid out in the SRG. There are now four levels of data that are used as the framework for authorizing cloud providers. They are IIL 2, 4, 5, and 6.

- All DoD data is important, but not all data needs to be equally protected
- Information Impact Levels (IILs) consider the potential impact should the confidentiality and integrity of the information be compromised

Once an organization understands their data level(s), they can accomplish market research to determine which Cloud Service Providers (CSPs) are authorized to provide Cloud Service Offerings (CSO)s for those levels. The CSPs are authorized through the FedRAMP process outlined below. The FedRAMP process is a cybersecurity process similar to the DoD's Risk Management Framework.

[8] Department of Defense, Cloud Computing Security Requirements Guide, March 6, 2017, https://iasecontent.disa.mil/cloud/Downloads/Cloud_Computing_SRG_v1r3.pdf.

IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	PERSONNEL REQUIREMENTS
2	PUBLIC or Non-critical Mission Information	FedRAMP v2 Moderate	US / US outlying areas or DoD on-premises	Internet	Virtual / Logical PUBLIC COMMUNITY	National Agency Check and Inquiries (NACI)
4	CUI or Non-CUI Non-Critical Mission Information Non-National Security Systems	Level 2 + CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical Limited "Public" Community Strong Virtual Separation Between Tenant Systems & Information	US Persons ADP-1 Single Scope Background Investigation (SSBI) ADP-2 National Agency Check with Law and Credit (NACLC) Non-Disclosure Agreement (NDA)
5	Higher Sensitivity CUI Mission Critical Information National Security Systems	Level 4 + NSS & CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal Systems Strong Virtual Separation Between Tenant Systems & Information	
6	Classified SECRET National Security Systems	Level 5 + Classified Overlay	US / US outlying areas or DoD on-premises CLEARED / CLASSIFIED FACILITIES	SIPRNET DIRECT With DoD SIPRNet Enclave Connection Approval	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal and Unclassified Systems Strong Virtual Separation Between Tenant Systems & Information	US Citizens w/ Favorably Adjudicated SSBI & SECRET Clearance NDA

Figure 4. Information Impact Levels (IIL)

First a CSP's Cloud Service Offering (CSO) has to be authorized to be able to provide services to the Federal Government through a program called Federal Risk and Authorization Management Program (FedRAMP https://www.fedramp.gov/).

- For cloud products and services used by the Federal Government, FedRAMP is the program that provides a standardized approach to:
    - Security assessment
    - Authorization
    - Continuous monitoring
    - OMB policy requires Federal departments and agencies to use FedRAMP approved Cloud Service Providers (CSPs) and share Agency ATOs with the FedRAMP Secure Repository. The concept is to "Do Once, Use Many Times". This means that each organization wanting to acquire cloud services from a CSP won't have to mandate that organization provide evidence that the company or organization complies with the applicable NIST security controls.
  - Once a CSP has successfully received a FedRAMP Provisional Authorization (PA) from a certified Third-Party Assessment Organization (3PAO), there is an additional step needed in order for the CSP to be able to provide services to DoD organizations for data at IIL levels above level 2. There are an additional 32-48 controls, depending on the Impact Level of the requirement, that have to be assessed for CSPs to be able to provide services for other than public facing data. If a DoD organization only requires services for data at IIL 2, then a FedRamp PA is sufficient to provide to an Authorizing Official to make an ATO decision.
- FedRAMP+ is the concept used in order to meet and assure DoD's critical mission requirements
    - Leverages FedRAMP assessment
    - Adds additional specific security controls and requirements (ranging from approximately 32-48 controls depending on the impact level)
  - DoD Provisional Authorization is an acceptance of risk based on an evaluation of the CSP's Cloud Service Offering (CSO) and the potential for risk introduced to the DISN
  - DoD PAs are granted by DISA to the CSP for a CSO, not for a CSP

- If a CSP's CSO (e.g., SaaS) leverages another CSP's CSO (e.g., IaaS) then the DoD PA for the former includes inherited compliance for the latter.
- The following web site is where the current status for CSPs are located: https://www.fedramp.gov/marketplace/compliant-systems/

Note: Security assessments performed under FedRAMP and FedRAMP+ do not include the DoD mission owner application residing in cloud services. Programs should plan to conduct cybersecurity test and evaluation of their application in the CSO environment under the contracted shared security model. For more information, refer to the DOD Cybersecurity T&E Guidebook v2, April 2018; Addendum: Cybersecurity T&E of DoD Systems Hosted on Commercial Cloud Service Offerings

3.2.1.3 Activity 3: Use Commercial Cloud Services that have a DoD Provisional Authorization (PA) and Obtain a Component Authority to Operate (ATO)

Each CSO must be granted a DoD PA in order to host DoD mission systems data. CSOs possessing a DoD PA are listed in the DoD Cloud Service Catalog. The responsible Authorizing Official leverages the DoD PA information for IIL levels 4-6 and the FedRAMP PA for IL 2, supplemented with an assessment of the risks within the Mission Owner's responsibility, in granting an Authorization to Operate (ATO). Authorizing Officials use the Risk Management Framework to issue an ATO. Figure 56 depicts this process from the top down.

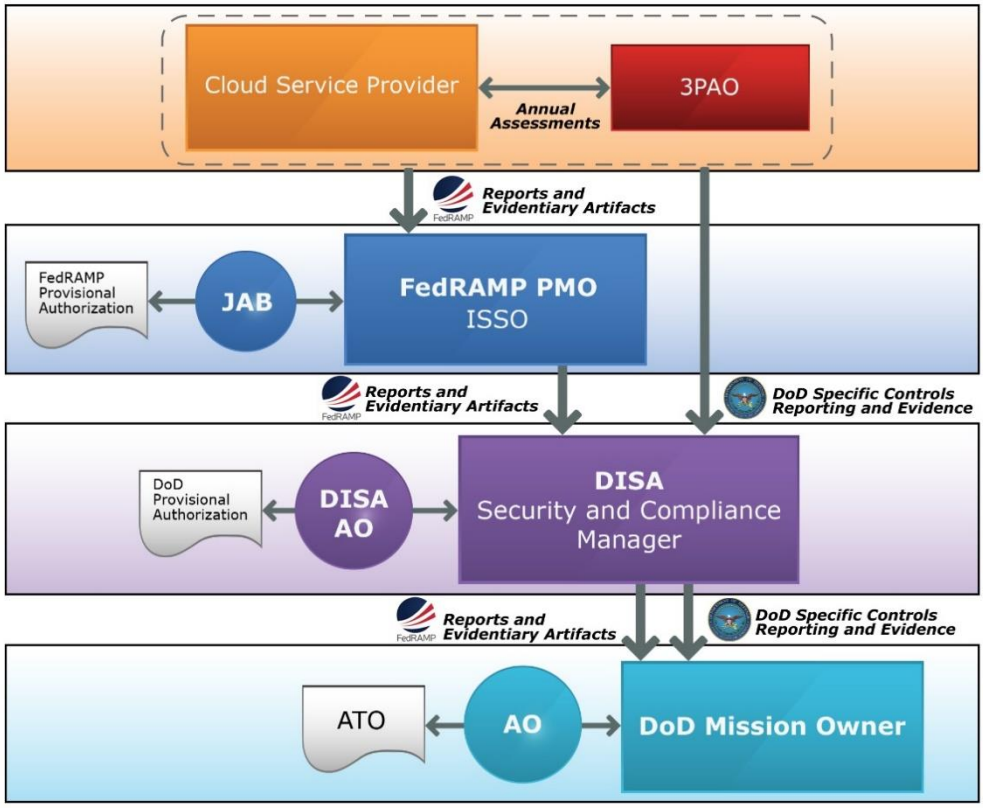


Figure 5. ATO Process

3.2.1.4 Activity 4: Use an Approved DoD Boundary Cloud Access Point (BCAP) and Cybersecurity Service Provider (CSSP) to Protect Sensitive Data

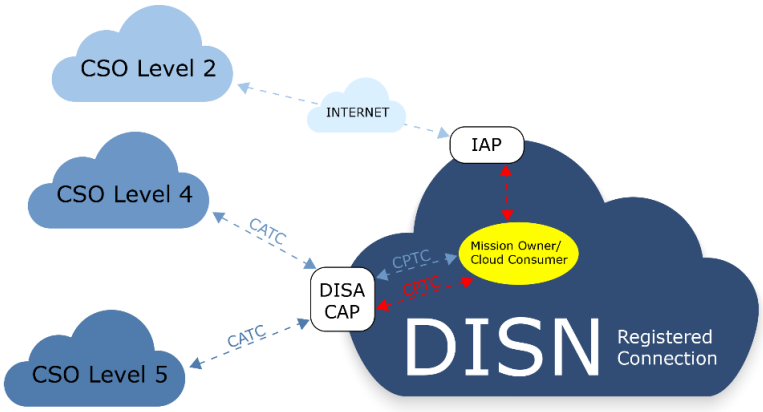


Figure 6. DoD Boundary Cloud Access Points

- A DoD Boundary Cloud Access Point (BCAP) is a system of network boundary protection and monitoring devices, otherwise known as an Information Assurance stack, through which CSP infrastructure and networks will connect to the DISN.
- With Controlled Unclassified Information data (Ireferred to as Level 4 and Level 5, a BCAP is required between the DISN and the CSO.
- The BCAP is used to protect the DISN, and systems, information and users residing on the DISN from attacks that may be launched from within a compromised CSO.The BCAP facilitates protected connections between users on a DoD network and systems/applications on the CSO.
- DoD BCAPs will provide the following generalized functions:
    - Intrusion Detection/Intrusion Protection
    - Data Loss Prevention
    - Full Packet Capture
    - Network Routing/Switching
    - Network Access Control to CSPs
    - Next Generation Firewall
    - Application Firewall
- The Cybersecurity Service Provider (CSSP) provides cybersecurity services and Command and Control direction addressing the protection of the network, detection of threats and response to incidents
- DoD PMs must ensure that CSSP processes are in place and functional for their application prior to any transition to or use of a CSO

3.2.1.5 Activity 5: Apply the Defense Federal Acquisition Regulation Supplement Rule to Commercial Cloud Contracts

- DFARS, Subpart 239.76 Cloud Computing
    - Policy and Responsibilities
        - Required storage of data within the US or outlying areas
        - Solicitation provision and contract clauses (252.239-7010)
- The contractor shall maintain within the United States or outlying areas all government data that is not physically located on DoD premises, unless the contractor receives written notification from the contracting officer to use another location.

- The contractor shall provide the government with a list of the physical locations which may contain government data within 20 days. Updates are required on a quarterly basis.
- The U.S. government restricts the transfer of sensitive or classified data (such as sensitive technology information and information that could potentially affect operational security) to locations outside of the control of U.S. companies or the U.S. government
- There are specific rules for the locations of data processing centers based on the IIL of the data:
    - IIL 2 and 4 must be hosted at locations in the U.S., U.S. territories, or on DoD premises per the Status of Forces Agreement (SOFA) unless the location is authorized by the AO
    - IIL 5 must be hosted at locations in the U.S., U.S. territories, or on DoD premises per the SOFA
    - IIL 6 must be hosted at locations authorized for classified processing

Note: Appendix A: Representative Example Contract Clauses provides additional contracting clauses and language that may be applicable to an organization's cloud acquisition.

3.2.2 DoD Secure Cloud Computing Architecture (SCCA) and DISA's Secure Cloud Computing

The DoD Secure Cloud Computing Architecture (SCCA) provides a standard approach for boundary and application level security for impact level four and five data hosted in commercial cloud environments.

The portfolio includes four services: boundary, application, and management level security capabilities with onboarding and service requirements found at https://www.disa.mil/About/Our-Work/Mission-Partners.

More technical details on SCCA and the DoD Cybersecurity Reference Architecture can be found in Sections 4.3.5 and 4.4.

4 Information Tailored for Specific Roles and Responsibilities

4.1 Program Managers Roles and Responsibilities

4.1.1 DoD Cloud Computing Strategy

Program Managers should read and understand the DoD's Cloud Strategy published in December 2018 in order to understand the DoD strategy moving forward. (See Appendix F: References)

The overview states the DoD's Cloud Strategy "outlines a path forward to an achievable objective: A Department-wide enterprise cloud computing ecosystem that allows us to revolutionize how we interact with technology every day. We will establish a multi-vendor, multi-cloud ecosystem that includes a combination of General Purpose (GP), Fit-for-Purpose (F2P), and Internal cloud environments hosted on and off premises across all classification levels. This will lay a foundation that will allow the DoD to maintain strategic advantage and information superiority and to fight with speed and agility by harnessing the power of the Department's data and systems. This is the realization of cloud computing: the ability to do more with more—to organize, analyze, secure, scale, and ultimately capitalize on critical information."

The strategy also provides a vision for how the DoD is moving forward with an enterprise GP cloud pathfinder called the Joint Enterprise Defense Infrastructure (JEDI) Cloud. From an acquisition perspective, this will be a single award Indefinite Delivery/Indefinite Quantity (IDIQ) contract and is currently planned to be awarded in CY19. More information on JEDI is found in this Guidebook in Section 6 Existing DoD Contracts and POCs. It should be clear that the DoD cloud acquisition strategy is more than just the JEDI pathfinder contract.

The diagram below depicts the strategy for moving from the current disjointed state to an optimized enterprise cloud environment. It identifies the assessments that will need to be performed, including both systems currently in cloud environments as well as those in physical DoD data centers.

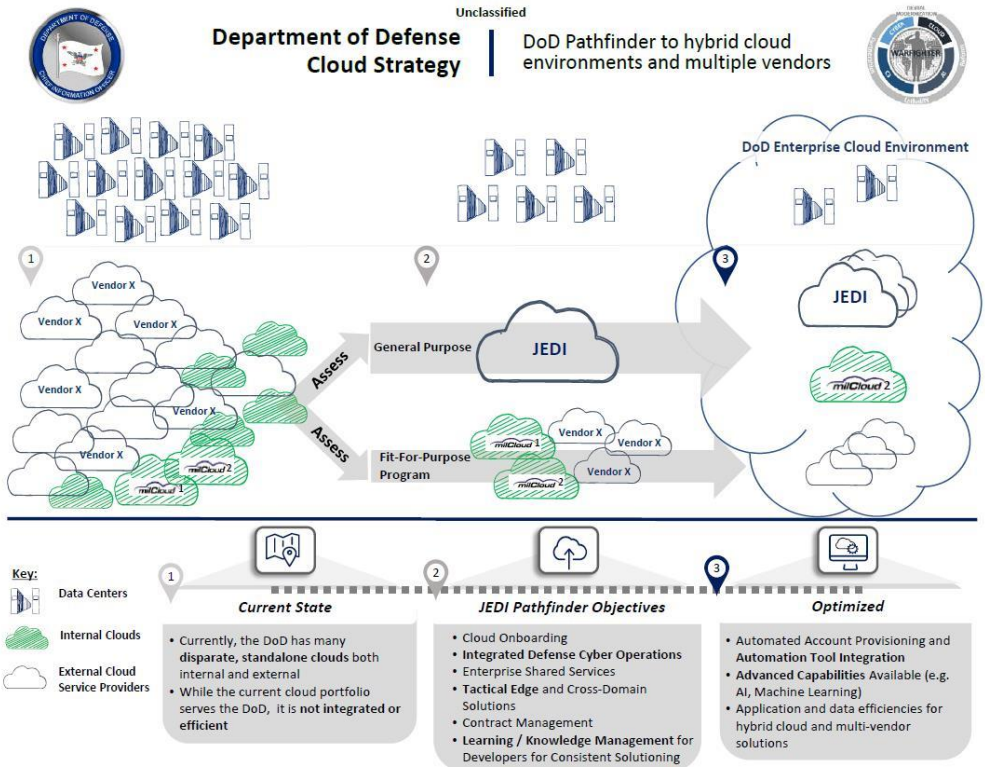


Figure 7. DoD Pathfinder to Hybrid Cloud Environments and Multiple Vendors

4.1.2 Best Practices for PMs Acquiring Cloud

In addition to the DoD CIO required 5 activities listed in Section 3DoD Approach for Acquisition of Commercial Cloud Services and the strategy briefly discussed above, the following is a list of activities recommended for PMs in acquiring cloud services.

1. **Select the appropriate Cloud Service type:** Choose the appropriate cloud service type and deployment model based on a complete understanding of your requirements and especially data impact levels. Is the requirement for IaaS, PaaS or SaaS? Is the requirement for a private cloud, public cloud, hybrid cloud? Is your data requirement at IIL 2 (Low/Public) or IIL4/5?
2. **Understand CSP and End-User Agreements**: Terms of Service and all CSP/customer required agreements need to be integrated fully into cloud contracts. There are several places in this Guidebook to find suggested contract language to meet specific requirements.
3. **Define a Service Level Agreement (SLA) or use SLA within a PWS as a Service Delivery Summary**: SLAs need to define performance with clear terms and definitions, demonstrate how performance will be measured, and what enforcement mechanisms will be in place to ensure SLAs are met. Appendix B: Example Service Level Agreement (SLA) Checklist provides a comprehensive SLA checklist to aid in defining service levels.
4. **Define CSP, Agency, and Integrator Roles and Responsibilities**: Careful delineation between the responsibilities and relationships among the DoD agency, integrators, and the CSP are needed in order to effectively manage cloud services. This is especially true for Cybersecurity Service Provider (CSSP) roles and responsibilities. More information on recommendations for those roles can be found in Section

4.4 Cybersecurity Considerations.

5. **Define Standards:** The use of the applicable cloud reference architectures and standards is necessary. The Guidebook references existing architectures and standards and well as emerging standards for cloud computing.
6. **Plan Early for Security**: Agencies must clearly understand the DoD Cloud Computing Security Requirements Guide (SRG) in order to plan early for security. Use this guidance to clearly detail the requirements for CSPs to maintain the security and integrity of data existing in a cloud environment. Use the Cybersecurity T&E Addendum: Cybersecurity T&E of DoD Systems Hosted on Commercial Cloud Service Offerings to plan for cybersecurity testing of applications as they migrate to the cloud.
7. **Plan Early for Privacy**: If cloud services host "privacy data," agencies must adequately identify potential privacy risks and responsibilities and address these needs in the contract. The protection of personal data, often referred to as "privacy," primarily relates to the collection, storage and use of personally identifiable information (PII). PII is any information that (a) can be used to identify the natural person to whom such information relates, or (b) is or might be directly or indirectly linked to a natural person. Again, the DoD Cloud Computing SRG is the source document to use to plan for privacy considerations.
8. **Ensure E-Discovery is Possible**: DoD agencies must ensure that all data stored in a CSP environment is available for legal discovery by allowing all data to be located, preserved, collected, processed, reviewed, and produced;
9. **Ensure Freedom of Information Act (FOIA) Compliance**: Federal agencies must ensure that all data stored in a CSP environment is available for appropriate handling under the FOIA; and
10. **Ensure E-Records Compliance**: Agencies must ensure CSP's understand and assist Federal agencies in compliance with the Federal Records Act (FRA) and obligations under this law.

4.1.3 Training Considerations

It is vital that DoD program teams have Government personnel that have a solid understanding of cloud computing. The Government has to put the requirements together, define the service levels, select a vendor and accomplish surveillance of the contractor. The following provides a list of training for various cloud computing services, platforms or technologies. It is not intended to be a complete and exhaustive list, but to introduce the reader to the breadth of options, programs and career growth paths in cloud technologies that may be pursued.[9]

Table 6. Training Websites

Offering	Program Type	Website URL
A Cloud Guru	Training and Certification Prep	https://acloud.guru/
AWS Training and Certification	Training and Certification Prep	https://aws.amazon.com/training/
Azure Training and Certification	Training and Certification Prep	https://www.microsoft.com/en- us/learning/azure-training-certification.aspx

[9] Copyright © 2018 Cloud Standards Customer Council

Table 6. Training Websites

Offering	Program Type	Website URL
Cisco CCNA Cloud Training	Training and Certification Prep	https://www.cisco.com/c/en/us/training- events/training-certifications/certifications/associate/ccna- cloud.html
Cloud Academy	Training and Certification Prep	https://cloudacademy.com/product/courses/
Cloud Credential Council	Training and Certification Portal	https://www.cloudcredential.org/
Cloud Institute	Certification Exams	http://cloud-institute.org/
Cloud Security Alliance	Training and Certification Prep	https://cloudsecurityalliance.org/
CompTIA Cloud Essentials	Certification Exam	https://certification.comptia.org/certifications/cl oud-essentials
Defense Acquisition University CLE075	Introduction to Cloud Basics	https://www.dau.mil
(ISC)^{2}Cloud Security Training and Certification	Training & Certification Program	https://www.isc2.org/Certifications/CCSP
OpenStack Training Marketplace	OpenStack Training Provider Portal	https://www.openstack.org/marketplace/training/
Oracle Cloud Training and Certification	Training and Certification	Training: https://education.oracle.com/training-by-product Certification: https://education.oracle.com/certification
SANS Cloud Security Training	Cloud Security Training	https://www.sans.org/course/cloud-security-fundamentals

4.1.4 Tracking DoD Cloud Program Activities

PMs must ensure they accomplish all required reporting activities when acquiring cloud services.

- SNaP-IT. Obtain an account for the DISA Select & Native Programming Data Input System for Information Technology (Snap-IT) database. Follow guidance for providing updates for cloud computing and cloud migration budget information.
- SNAP. Obtain an account to DISA's Systems/Network Approval Process (SNAP) system to manage cloud computing implementations with commercial clouds. This provides visibility into runtime cloud use within DoD and is critical for SA of where data is located in cloud environments.
- eMASS. Ensure your Cloud acquisition information is put into the Enterprise Mission Assurance Support Service (eMASS) system IAW all DoD Risk Management Framework (RMF) policies and guidance.
- Complete Cloud Service Offering funding reporting responsibilities, e.g., SNaP-IT, Budget 300 Exhibits 53A/C (or current reporting requirements).

4.1.5 General Cost Considerations in Commercial Cloud Environments

The following table outlines several areas to consider when acquiring cloud services. It is crucial to understand how these services are deployed and operated in order to avoid paying for services not utilized.

Table 7. Explanation of Cost Drivers in Cloud Environments

Cost Driver	Consideration
Over-Provisioning	Over-provisioning is when demand for an application is overestimated. Cloud service providers make it easy to max out and the costs become inflated. Although servers can be scaled back, this is a slow process and until that happens costs are over-inflated. Ways to decrease costs include: • Ensure virtual instances are shut down when not in use. • Understand uptime requirements and scheduling and monitor usage.
Under-Provisioning	Under-provisioning is when demand is underestimated. It is easier to detect and fix since it means the cloud service's performance is not acceptable.
Spin It Up, Then Forget It	Having too many admins in the cloud is costly since they do not always communicate with each other and server instances are then spun up for a particular purpose that is never used. A tremendous amount of money can be saved and security can be improved by **turning off resources** that are no longer needed.

Table 7. Explanation of Cost Drivers in Cloud Environments

Cost Driver	Consideration
Storage Choices	Many cloud service providers offer different tiers of storage pricing based on how accessible the data is. Standard storage is frequently accessible, yet the most expensive. Then there's a semi-accessible tier, and also an infrequently accessed tier for data you want to keep but expect to rarely need access to. Organizations need to think carefully about which tier structure they need for specific data. Since **storage grows and never shrinks** storage consumption should be actively managed by moving data to lower cost services when they are no longer in constant use, leveraging caching and deleting unneeded files.
Free (With Strings Attached)	The "free tier" is still billable if its thresholds are exceeded and this happens frequently without the admin realizing they've gone way over what the free tier allows. Some free cloud offerings also have an expiration date after which the full-rate billing begins.
Appliance Charges	Some cloud providers offer a menu of different virtual network and server instances that can be "rented" (e.g. load balancers, VPN concentrators and databases) but unless the exact frequency of usage is known, choosing a size and payment model can be challenging and will lead to higher than necessary costs.
Free To Enter, Pay To Leave	It is never a good idea to shop for a cloud provider when IT needs are high and timelines are tight because it may lead to selection of a cloud provider that is costly and the data that was moved into the cloud for free may cost an arm and a leg to extract and move to a competitor.
Troubleshooting Complexities	Troubleshooting is typically an overlooked cost that becomes more time consuming and expensive overtime. The root cause of complex technical issues is challenging to resolve because there is often no visibility into a cloud and in-house staff must work with the service provider to resolve issues.
SaaS	SaaS services nearly always carry a perpetual, per-user license (paid monthly on an annual or multi-year term). Hidden costs include: 1. **Customization** – To lower costs, SaaS should be used as it was designed. Customization will lead to unanticipated development and maintenance costs. 2. **Integration and Testing** – SaaS will inevitably be integrated with in-house apps, data stores and other SaaS services. Best practice is to define an integration architecture with as simple a business process as possible, then test the integrated services to understand capabilities and security features 3. **Sprawl** – Access to SaaS apps must be carefully monitored. Most vendors have volume pricing for SaaS, meaning the more units purchased, the less per unit cost.

Table 7. Explanation of Cost Drivers in Cloud Environments

Cost Driver	Consideration
Not Activating Cloud Economics for Applications	Not every app fits with a pay-per use platform. The best take advantage of the pricing model and include: 1. **Elastic Scale** – The app increases or decreases its resource consumption based upon usage. 2. **Transient Apps** – That can be parked or shut off when not in use (e.g. batch work, high performance computing, seasonal apps), rather than one that sits there 24/7 consuming the same resources.
Data Consumption	Data consumption is the biggest cost driver. Cloud-based apps should be regularly optimized for better database performance (such as storage architecture and query optimization/plans) or they end up using unnecessary resources and increase costs.

4.1.6 DoD-Specific Cost Considerations for Commercial Cloud Environments

Trying to acquire cloud services within the constraints of the FAR and other DoD specific regulations is difficult because Government/DoD systems were not designed to accommodate the variable usage and quick-pay cycles that are the hallmark of the commercial cloud computing models. This is especially true for business systems.

Unlike business-to-business contracts, Government contracts are constrained by fiscal laws. The Government cannot incur obligations in excess of contract funding, nor can the Government front-load funding for more support and services than are expected. With few exceptions, the Government cannot pay for services in arrears. To cope with quick usage to bill cycles, the Federal Government must obligate money commensurate with current federal law which requires agencies to either set aside a large amount of money for corresponding services it may never fully consume or set aside a little money that may not cover its actual service consumption. The Federal Government does not currently have access to usage-to-quick-payment capabilities in its policies and systems. As a result, it currently accepts a set of funding mechanisms that risk overspending for those services or routinely accepts risk of anti-deficiency. The current mechanisms of Federal funds systems work directly against the intended business advantages of cloud computing. This is the most impactful issue facing the Federal Government with cloud computing. While there are other disadvantages in the current Federal structures, they generally have a much lower impact than funding constraints.

Table 8. Funding Cloud in Private and Public Enterprises

Funding Cloud in Private Enterprise	Funding Cloud in Public Enterprise
Pays for cloud with “consumption-based” model using metered billing	Constrained by budgeting and spending regulations and cannot utilize true “metered” services

Table 8. Funding Cloud in Private and Public Enterprises

Funding Cloud in Private Enterprise	Funding Cloud in Public Enterprise
Flexible budgeting cycles and methods	Restricted budgeting based upon Fiscal Year.
Utilize business-to-business contracts that allow for front-loading and cost overruns	Cannot incur obligations in excess of contract funding
Ability to move funds easier to cover costs of demand surges or quick scaling	Must obligate a set amount of funds that may not cover full demand or may overestimate and leave money on the table

To solve the funding challenge, this Guidebook recommends a set of actions to mitigate these disadvantages. Most importantly, it recommends the use of Time and Materials (T&M) type contracts for cloud computing contracts, and a clarification of T&M contracting within the Federal Acquisition Regulations (FAR). Specific approaches, pros and cons, and additional details are located in Section 4.2.3 Paying for Cloud.

4.1.7 Data Ownership and Data Breach in the Cloud

4.1.7.1 Data Ownership

Another critical requirement is ensuring that the agency acquiring cloud services retains ownership of the data it stores and the rights to access, modify, or migrate that data if and when it chooses. Such an agreement ensures that the Government can select and migrate to another CSP if it is not satisfied with the services it receives. This point must always be made clear with the CSP prior to the acquisition and specified in writing in the final contract.

4.1.7.2 Data Breach

Ownership rights are especially important to negotiate beforehand to address potential data breaches. It is a best practice to ensure that the CSP is held accountable for data breaches, even as they do not own the data. According to the CIO Council and the Chief Acquisition Officers Council, “Federal agencies should make explicit in cloud computing contracts that CSPs indemnify Federal agencies if a breach should occur and the CSP should be required to provide adequate capital and/or insurance to support their indemnity. In instances where expected standards are not met, then the CSP must be required to assume the liability if an incident occurs directly related to the lack of compliance.”[10]

Greater detail on data ownership and rights pertaining to termination of service, breaches, and information and

[10] “Creating Effective Cloud Computing Contracts for the Federal Government.” February 2012. https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf

records management can be found in the CIO Council report.[11]

4.1.8 Risks of Not Buckling Your Seatbelt

This document details many of the capabilities and benefits such as the rapid elasticity and scalability of cloud computing. There is little “friction” to adding more resources near-instantaneously when they are needed. There is often an Application Programming Interface (API) for automated approval, taking the human aspect out of the equation and expediting the approval for scaling. The speed of the scalability can be a massive benefit to the consuming agency. An API is the part of the remote server that receives requests and sends responses.

While this scalability is most often a benefit, there are also potential pitfalls. Cloud often relies on decentralized responsibilities meaning that the ordering capability (deployment of each cloud resource) is broadly distributed and potentially automated. The agency must consider how to potentially manage many cloud resources individually and consider demand at the aggregate agency level. Each cloud resource that is ordered is committing the government to paying for that resource with costs accruing as soon as that resource is requested and deployed. There is no way to stop the resources from being ordered when rapid scaling takes place. In extreme cases, this could put the agency at risk of violating the Anti-deficiency Act by incurring obligations or making expenditures that exceed the amounts available in appropriations or obligations.

Additionally, these resources are quickly spun up are sometimes not spun back down, leading to wasted resources and unnecessary expense. Easy scalability without proper governance can lead to the government committing to a large sum of money. There can be instances where scaling up for resources are outside the IT security boundaries - an agency’s authority to operate (ATO). In these cases, the speed that is usually considered a benefit is now a detriment.

These risks can all be mitigated by having the proper governance structure with the responsibility to enable IT cloud solutions and cloud related programs within the acquisition and contracting policies. Proper governance is required to mitigate the risk of violating the Anti-deficiency Act should an agency run up charges that are in excess of what has been obligated. A strong governance structure establishes consistent interpretation of policy and monitor cloud performance while addressing potential consumption issues. In addition, this governance reduces or even eliminates investments that are underutilized (e.g., pilot programs that are no longer used). For example, the governance model may outline how the CSP can provide alerts at a predetermined level of consumption to avoid invoices exceeding their budgeted amount.

4.2 Contracting Officers/Financial Managers/Attorneys

It is critically important that the contracting officers, financial managers, and attorneys advising programs understand the specific considerations for acquiring cloud computing services. The following sections provide guidance in several areas to assist Contracting Officers (COs) and Attorneys in understanding these specific topics.

4.2.1 Choosing a Requirements Document Type

[11] Ibid.

Cloud computing requirements documents can be variously crafted as either a Statement of Objectives (SOO), a statement of work (SOW), or a Performance Work Statement (PWS).

Agencies often use a PWS by default. This is true for services because performance-based acquisition (see subpart 37.6) is the preferred method for acquiring services (Public Law 106-398, section 821). This requirements document is consistent with FAR guidance and normally provides an exceptional opportunity to obtain necessary services with demonstrable outcomes. The PWS is not always the best choice and in some situations when acquiring cloud services other options may be better suited. The more familiarity an agency has with cloud acquisition in combination with its IT acquisition maturity level, the more likely the agency can successfully leverage a PWS. To understand and grasp the nuances requires great familiarity with cloud computing along with the scope and intended uses of the acquisition.

Many agencies use a SOO which states the agency goals in the most general sense, allowing vendors more creativity in proposing a solution. For instance, instead of naming the number and type of processors needed, the amount of memory and storage, etc., only the projected usage statistics of an application are named. Usage statistics such as the number of visits to a website per day, the average page size, the average number of pages viewed per visit, etc., are provided in a SOO.

Table 9. Requirements Document Type Benefits

Requirements Document Type	When to Use and Benefits
Statement of Objectives (SOO)	• States performance objectives and constraints (e.g., security or availability), but is not prescriptive on "how" the work should be accomplished • Allows vendor creativity in proposing solutions • Good to use when agency can provide usage statistics and has no preferred or mandated way of providing the service • Usually shorter than SOW or PWS
Statement of Work (SOW)	• Tells vendors what to do and how to do it; most prescriptive type • Good to use when there are very specific requirements and constraints that limit the flexibility of potential solutions
Performance Work Statement (PWS)	• Similar to SOW, but contains no "how-to" statements; lists requirements and constraints • Not as flexible as SOO, but not as prescriptive as SOW

In general, for cloud computing, a SOO issued within an RFP would suffice. That way, the vendor solutions contained in responses can be innovative yet contain specific pricing. If the agency wishes simply to establish an agency "gift card" type of drawdown account with funding attached to a CSP then this may be an optimum solution. CSPs may respond with their full price list of available services, which the agency can pick and choose from at the task order level. Since this could be extremely difficult to evaluate and defend a potential protest, the acquirer may want to use sample task orders as a means of level setting for purposes of evaluation.

The final selection of the SOO, SOW, or PWS is authorized by the ordering CO based on the characteristics of the acquisition. It is important for the IT shop or program office to engage with their CO early in the process because decisions like these need to be made throughout this process. For example, a SOO may allow the vendor to provide more innovative solutions, but they are difficult to evaluate since CSP offerings are often quite different. A PWS may still be able to be used at the high level with just the end state defined. That will still allow for innovation solutions to be proposed.

4.2.2 Cloud Service Models and Contract Types

There are three service models as defined by NIST: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), as defined in section 2.2. These service models are vastly different in use characteristics from the consumer standpoint. As such, these models may require different approaches to be better managed and paid for under different conditions or contract types. The two most common contracts types for cloud service models in the Federal Government are Time & Material (T&M) and Firm Fixed Price (FFP). T&M is still the least preferred method of contracting since the contractor has no incentive to control costs (FAR 16.01). Therefore, the Government is required to provide surveillance which may or may not be possible as well as write a Determination and Findings (D&F) as to why this contract type was chosen.

Consider the service models required; and then determine the subcategories of those service models. Consider IaaS and PaaS together, and SaaS on its own. The two subcategories to consider under IaaS-PaaS are whether or not IT professional services are needed in support of the service model. For SaaS, consider the subcategories as seats and usage, but IT professional services are still an important consideration depending on the service. This sets up a framework for an appropriate discussion of cloud service models and contract types. An additional consideration for contracting officers is to understand technical responsibility and writing that into the contract. In the SaaS model the CSP is responsible from the application layer all the way down the stack. Also, in the SaaS model or subscription model the agency needs to budget for the service. In IaaS or PaaS, you bring your own licenses and may or may not update them depending on funding.

Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) share characteristics such as application hosting replacements for traditional servers housed in an agency's data center. In a subscription-based model a fixed amount of computing services is bundled together, and the agency is charged monthly. For agencies procuring IaaS and PaaS without professional services, a FFP contract should be used. Contract risk should be relatively low and predictable within acceptable limits. The vendors and agency can reasonably agree on price. This does not come without risk as agencies can be charged for services not used or are charged more than expected (neither scenario takes advantage of pay for use promised by a cloud solution). In cases where agencies require support services, they should consider a T&M CLIN separate from the IaaS and PaaS FFP CLINs and identify their requirements for the CLIN. Agencies can avoid these risks by writing in broad CLINs that provides the customer flexibility. A broader scope alleviates Government concerns around exceeding categorized line items within a contract.

SaaS offerings vary from IaaS and PaaS in that vendors typically charge for active users or seat licenses that are permitted to access the service. SaaS seats may be scaled up or down each month in keeping with the metered billing model for use in a T&M or FFP contract. To take advantage of the SaaS cost savings, a T&M contract type should be used to pay for usage. Most SaaS offerings include monitoring capabilities built into the service. Agencies can take advantage of the automation tools to help provision, control access, and provide

cloud monitoring and reporting. It may be difficult to get agency CO buy-in as the FAR imposes limitations on T&M contracting. If an agency selects an FFP contract type for a SaaS procurement, allow for the flexibility at the CLIN or TO level so cost savings can be realized.

Table 10. Service Model Contract Type Considerations

Service Model(s)	FFP Considerations	T&M Considerations
Infrastructure as a Service (IaaS) Platform as a Service (PaaS)	• Use when no professional services needed • Use when vendor and agency agree on price	• Use when support services required (should be separate from FFP order) • Identify support needs in CLINs
Software as a Service (SaaS)	• May be favored by agency CO • Needs to allow for flexibility at CLIN or TO level to enable savings • Limit to seat-oriented contracts	• Usually used for SaaS • Enables better cost savings • May be difficult to obtain CO buy-in

Support requirements for all contracts will include items such as system integration and Test And Evaluation (T&E) requirements. For more information, refer to the DOD Cybersecurity T&E Guidebook v2, April 2018; Addendum: Cybersecurity T&E of DoD Systems Hosted on Commercial Cloud Service Offerings.

In summary, T&M is the appropriate contract type for IaaS-PaaS if labor is required; otherwise, FFP is more advantageous. For SaaS, T&M is useful in all cases including seats and usage, but FFP should be limited to seat-oriented contracts and include options based on tiers of usage.

4.2.3 Paying for Cloud

4.2.3.1 Consumption-based Billing

The metered billing aspect of cloud computing services is a critical element to achieve the goal of improving IT spending efficiency. Consumption or usage-based billing is the most desired payment method for cloud computing to drive down costs for the government and to create the most efficient spend. Vendor billing for cloud computing power is often metered and broken down into units of processing power, units of storage, and units of up/down bandwidth, all by the minute or hour.

This form of billing is widely used in the private sector but is not common among government customers. Metered cloud computing billing with cost benefits conveyed by buying only the amount required causes confusion and concern in the government contracting community. The challenge contains aspects of both contracting specifics and government financial business processes. Consumption-based billing is burdensome in terms of the management required to budget, obligate, and monitor billing.

4.2.3.2 How the Government Pays for Cloud

Cloud computing services clearly fall within the realm of commercial services, and there are numerous pricing

models for cloud in the commercial world. However, unlike business-to-business contracts, Government contracts are constrained by fiscal law. The Government cannot incur obligations in excess of contract funding. Nor can the Government front-load funding for more goods or services than is reasonably expected. This is problematic when unexpected demands (e.g., disasters, recovery services, etc.) emerge.

If an agency discourages the use of T&M contracts because of the risks to the Government, how will a contract be crafted when the method of billing calls for a T&M contract type? There are risks of running out of funding and violating the Antideficiency Act, especially for a service that can be easily provisioned. Most agencies' innovations with respect to procuring cloud computing services have relied upon flexibilities already existing within the FAR. Agencies are using three approaches for paying for cloud computing services today, including:

- Approach 1: Optional CLIN Not to Exceed (NTE)
- Approach 2: Drawdown Accounts
- Approach 3: Subscription Based

For Approaches 1 and 2, agencies manage the risk of runaway cloud services and labor exceeding funding, and possibly violating the Antideficiency Act, by crafting a per unit of sale Firm Fixed Price (FFP) contract and then monitoring the burn rate similar to a T&M contract. Excess funding may need to be de-obligated near the end of the fiscal year. Agencies must have contract management governance in place to monitor cloud services contracts. Many CSPs offer tools that will alert agencies when a specific threshold of spent funds has been reached to help mitigate this situation.

The third option available from CSPs is offering cloud services by subscription. Rather than paying by the individual item, a CSP might offer a bundle of cloud computing services for a fixed monthly price that the agency must commit to using for a defined period. The agency then receives a known quantity of cloud services for a known price for many months, or even a year. The agency has some risk since the subscription cloud services are provided on a "use or lose" basis where the agency might pay for unused computing power that it has committed to via subscription. In this case, the agency forfeits one of the advantages of cloud computing - its potential for saving money during periods of low consumption. The other advantages of cloud computing, such as agility, etc., are not affected by the subscription billing model.

Each of these approaches is described below along with an explanation of their disadvantages and why they are preventing the government from acquiring cloud services.

Approach 1: Optional CLIN Not to Exceed

A contract contains one or more optional CLINs specific to the hosting of cloud computing services. The government obligates the money to a CLIN as needed and the funded vendor does the work based on a notice to proceed. The government receives invoices as the services are consumed and the vendor is paid out of the obligated money. The government monitors the bucket of money and exercises another optional CLIN as necessary to support additional cloud computing utilization.

Pros: Most common method for funding cloud and is the traditional method on contracting for IT services.

Cons: Unable to ramp services up and down based on usage. There is not full realization of the benefits of elasticity of cloud in terms of cost savings.

Approach 2: Drawdown Accounts

Drawdown Model A: Government monitors

The government engages with the vendor to estimate what the government is going to use. The government agrees to terms with the vendor such as $50 million over 5 years, which comes to $10 million per year. The government obligates the initial $10 million annual amount. Each month there is a bill and the money is taken from the fund to pay it. There is a drawdown against that account. The remaining funds are monitored for burn rate. If the remaining funds get low, the agency requests additional funds from the CFO that can be obligated to maintain services.

Drawdown Model B: Vendor monitors

The vendor is obligated a lump sum of money for work to be completed. The vendor keeps track of burn rate and value. There is a drawdown against that account. Once the burn hits a prearranged level such as 70%, the vendor notifies the government and estimates how long 30% remaining will last. The government obligates additional funding to “recharge the debit card” and work proceeds.

Drawdown accounts are just another name for process steps that necessarily occur when the government contracts for goods and services.

Pros: Allows customers to realize elasticity and flexibility benefits of cloud services.

Cons: Burdensome bookkeeping and effort for either the CO or the vendor as usage can be unpredictable.

Approach 3: Subscription Based

Under the subscription model of CSP billing, a fixed amount of computing is bundled together for a recurring fixed monthly price. The agency may consume all or part of the bundled computing resources each month. If the agency does not use the entire bundle during the month, the remainder is lost. Thus, an agency which awards a FFP contract for cloud computing receives the benefit of knowing exactly how much each monthly invoice amount will be. But through the “use or lose” aspect of this contract type, the agency may not realize the “pay only for what you use” cost savings benefit of cloud computing metered billing.

The government determines upfront what the needs will be and obligates the money to fund that level. The overall number is divided by 12 to determine the monthly amount to be paid. Each month there is a standard invoice of 1/12th of the funding at set invoice level. The government goes into it knowing that they will pay for 10k units each month whether they fully use it or not.

Pros: This option works well if the hosting options are consistent throughout the life of the contract. There is low risk, a certainty of forecasted utilization, and is relatively simple to execute.

Cons: Government will typically add a buffer which ends up leaving money on the table. The CO obligates $100k per month for what should be $60k. This method nullifies the purpose of cloud allowing payment for what is actually consumed.

Conclusion

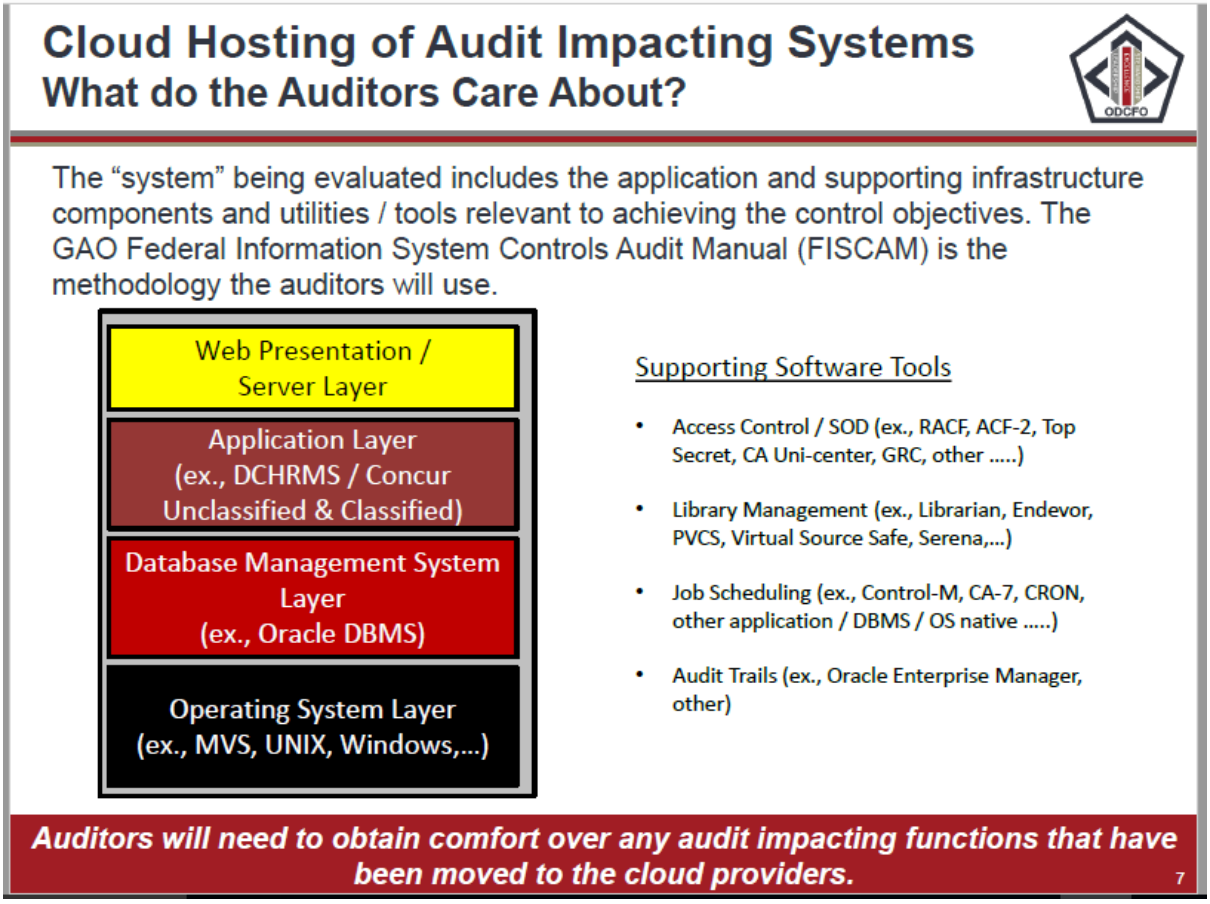
The Federal government’s existing methods of buying cloud services (i.e., optional CLINs, drawdown accounts, and subscription models) do not effectively address the problem of demand elasticity and portability. They are

ultimately minor variants in contracting structure, business financial process emphasis, or product re-characterizations that only help incrementally by shifting trade-offs without providing complete solutions. None of these methods provide for a complete realization of benefits of cloud computing by providing effective means for the government to both consume and pay only for the resources it needs and uses. A potential solution to this might explicitly allow for cloud computing resource units to be treated, including associated oversight risk, like labor hour rates (fixed unit price) in T&M contracts.

4.2.3.3 Cloud Specific Financial Audit Requirements

Programs are required to comply with financial audit requirements. In March 2019, the Office of the Under Secretary of Defense (Comptroller) released the Financial Statement Audit Requirements for Service Organizations (DoD Cloud Way Forward). Reference is listed in Appendix F.

The reference document clearly describes how technical “audits” or reviews such as FEDRAMP or RMF are not sufficient for the purposes of financial audits. An excerpt is below:



Also ensure compliance with the SSAE 18 and reporting requirements for Service Organization Controls (SOC) if required. Reference https://www.ssae-16.com/soc-1-report/the-ssae-18-audit-standard/.

4.2.4 Legal and Contractual Concerns

There are a host of important legal and contractual clauses to consider when selecting and acquiring a cloud service. To fully utilize Federal best practices and lessons learned and to simplify the acquisition process, refer to the report by the CIO Council and the Chief Acquisition Officers Council, "Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service." [12] This document contains a substantial amount of useful information and should be an agency's first resource on legal and contractual topics such as:

- CSP and End User Agreements
- Cybersecurity test and evaluation support
- Service Level Agreements
- Privacy
- E-Discovery
- FOIA Access
- Federal Recordkeeping

An additional reference tool in use in support of proper clause development is located in Appendix A: Representative Example Contract Clauses.

4.2.5 Strategic Contracting Considerations

While the scenarios in this Guidebook used an assumption of a single contract to procure and execute the entire scenario, there are many other contracting permutations that agencies might leverage in their cloud environment. The types of services that providers offer to organizations will continue to grow. One option to consider is to use multiple procurements to separate the cloud professional services from the hosting services. Doing so allows agencies to swap out CSPs without interrupting the work being done by the cloud professional services contractor or vice versa preventing vendor lock-in. Of course, multiple acquisitions come with their own challenges and many programs want to use one contract to manage their cloud services. For example, it would be wise to choose vendors with open source technologies or to use contracts that cover the breadth of the total solution. The Government Services Administration (GSA) offers total solutions using Federal Supply Schedules.

[12] "Creating Effective Cloud Computing Contracts for the Federal Government." February 2012. https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf

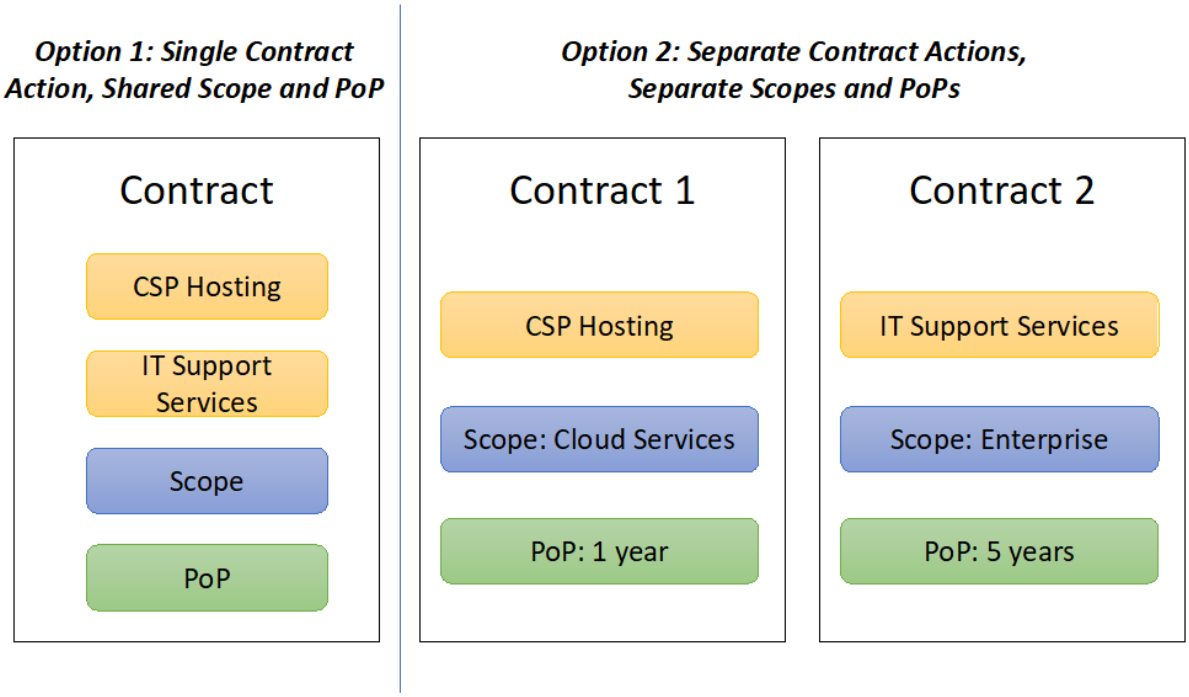


Figure 8. Contract Options Representation

Cloud application architecture provides additional options to enhance enterprise agility in contracting for cloud IT services. Opportunities can exist or can be created through planning via enterprise architecture efforts within a cloud strategy, to strategically segregate the hosting and contracting of major components of IT systems. For example, a SaaS presentation layer might be separately hosted from the data store which undergirds the system. This would allow a potentially less complicated and less risky migration of a support contract from an underperforming vendor to a new contractor. Agencies could consider this multiple cloud strategy across other applications as well using a Cloud of Clouds approach allowing for a combined public and private cloud environment, as well as services and platforms from a diverse set of independent software vendors working harmoniously in this secure environment.

Government struggles with moving the critical mass of Government IT to the cloud and this, therefore, leaves most of the Federal legacy IT systems intact. Agencies face the challenging task of overhauling legacy systems to transition them to the cloud. One option is to adopt a hybrid approach where agencies strategically move all IT infrastructure to a Contractor Owned/Contractor Operated (COCO) model with cloud capability. This approach allows agencies to move all IT infrastructure to a contractor and immediately migrate all “cloud ready” systems and applications into a cloud environment. Agencies can then work with the contractor on a transition strategy, in a phased approach, to begin migrating legacy systems to cloud-enabled technology, or sun-setting them in a manageable timeframe with little risk if needed.

Agencies can also strategically segregate contracting actions, often based on hosting versus professional

services, by presentation layer versus data layer, or a combination of these approaches. By doing so, various risk tradeoffs are optimized to match individual organizational needs. It also allows agencies to take a more focused approach to each portion of their cloud acquisition strategy and as agencies gain maturity in the cloud, these approaches can be considered and tailored to maintain agility and responsiveness within IT.

Though there is a FedRamp clause and contracting language on the FedRamp site, for DoD contracts the DoD requires the DFAR clause be used. This clause links to the DoD Cloud Computing SRG which covers the FedRamp requirements.

Other strategic contracting considerations that should be addressed are:

- Availability and Availability Reporting of the Cloud Services.
- Service Interruption Reporting – The Contractor must inform the Government of any interruption in the availability of the cloud service as required by the service level agreement.
- Outage Estimate – Whenever there is an interruption in service, the Contractor shall inform the Government of the estimated time that the system or data will be unavailable.
- System Availability Requirements – The estimated timeframe for recovery of the service must be related to the FIPS 199 system categorization for the availability of the system, and if specified, the Contractor shall meet the agreed upon service level and system availability requirements.
- Testing – CSPs may place limitations on certain types of security testing in the CSO used by the Government. Programs should specify language in the RFP and contract to obtain the required T&E support. Programs should also ensure the SLA includes metrics to demonstrate via testing that the CSP is delivering the mission owner's required cybersecurity, survivability and operational resilience capabilities.
- The Contractor shall provide regular updates to the Government on the status of returning the service to an operating state according to the agreed upon SLAs and system availability requirements.
- Protecting of Government Data
- Protection of government data is required by the Federal Acquisition Regulations (FAR) procedures, guidance, and information (PGI)
- Data ownership, licensing, delivery and disposition instructions specific to the relevant types of Government data and Government-related data shall be part of the contract
- Appropriate limitations and requirements regarding contractor and third-party access to, and use and disclosure of, Government data and Government-related data shall be documented in the contract
- Appropriate requirements to support applicable testing, inspection, audit, investigation, or other similar authorized activities specific to the relevant types of Government data and Government-related data, or specific to the type of cloud computing services being acquired
- Appropriate requirements to support and cooperate with applicable system-wide search and access capabilities for inspections, audits, investigations, litigation, eDiscovery, FOIA requests, records management associated with the agency's retention schedules, and similar authorized activities
- A requirement for the contractor to coordinate with the responsible Government official designated by the contracting officer, in accordance with agency procedures, to respond to any spillage occurring in connection with the cloud computing services being provided
- A requirement that the Contractor shall use Government-related data only to manage the operational environment that supports the Government data and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer.
- Ensuring access to Government Data for Law Enforcement and Other Purposes
- Ensuring compliance of regulations for Government Records Management Policies
- Defining Service Levels (SLAs added to SOO/PWS or standalone). SLAs are important in a cloud environment since the organization is giving up control over certain aspects of their IT services.
- The SLA shall clearly define the contract performance standards, how the contractor will measure and report the service performance, and the enforcement mechanisms for SLA compliance.

- Ensure that the contract clearly specifies whether there are any maintenance windows when service can be disrupted and notification procedures for planned and unplanned outages.
- Clearly define any monitoring and metering requirements the organization has for monitoring the performance of the CSP and capturing the organization's usage patterns and for charging the organization's clients for services.
- Clearly defining Subcontracting Rules
- Ensuring proper Supply Chain Management
- Ensuring clear Terms of Service - Many commercial services have Terms of Service Agreements that contain clauses that the government cannot accept. Some common examples are below:
- Confidentiality. This is a clause where the government agrees not to release confidential information. However, the government is subject to the Freedom of Information Act and must follow its procedures to release or protect commercial information.
- Indemnification. Many terms of service agreement contain an open ended indemnification clause where the government will indemnify the CSP against third party claims. This type of clause violates the Anti-Deficiency Act because the government is committing to funds that have yet to be appropriated. This clause needs to be re-worked to reference other applicable laws. – Note: ALREADY in the DFARs CLAUSE
- Governing Law. Many terms of service agreements have the governing law for the agreement to be a specific state and have a venue for any disputes to be in that state's courts. As the Federal government is not subject to state law, it can only be sued in Federal court.
- Endorsement. Many terms of service agreements also have a clause where the CSP may quote / cite the government's use of its product as an endorsement or testimonial. The government does not endorse commercial products or services.

4.2.6 Blanket Purchase Agreements

Blanket Purchase Agreements (BPAs) are an important tool that can solve certain elaborate cloud computing challenges. A BPA, governed FAR 8.405-3 for GSA Schedule opportunities, is an administrative arrangement that provides a simplified method of filling anticipated recurring needs for goods and services by establishing an indefinite delivery indefinite quantity (IDIQ) instrument with those contractors who are qualified sources of supply. A BPA is not a contract and does not obligate funds. A BPA simply establishes the terms and conditions and pricing under which a purchase would occur including contract types and clauses.

BPAs provide for convenience, efficiency, and reduced costs as well as a simplified ordering process. Multiple agencies can band together to place orders for similar requirements. There is much less overhead relative to all agencies and agencies can increase their purchasing power to get volume discounts. BPAs offer shortened acquisition lead times and agencies can reuse or leverage requirements other agencies have already developed. BPAs formed under a GSA Schedule are not synopsized as part of the solicitation process. A BPA can be established with one Schedule contractor or multiple contractors in accordance with FAR 8.405-3, referred to as a Single-Award BPA or a Multiple-Award BPA. The preference (established through 8.405-3) is for multiple-award BPAs and leaves the discretion of number of BPA awards to the ordering activity and should be based on maximizing the effectiveness of the BPA(s).

IDIQs can apply across a host of opportunities and should be considered as a viable procurement strategy. For

example, the Army ACCENT[13] Multiple award IDIQ has many characteristics that fit a BPA procurement strategy such as recurring transition requirements. Army wanted a standard tool that preset all the base requirements for their estimated 10,000 applications that are to be migrated to the cloud. The contract requirements included IaaS, SaaS, and PaaS offerings and had offerors demonstrate a DISA issued Provisional Authority for award. It further included in scope all the IT professional services needed to fully support and execute the transition and migration of these applications. Although ACCENT was not itself executed as a BPA, it is an excellent example of a use case for a cloud BPA that includes migration services in contrast to the DHS ECS BPA which is limited to CSP services.

When establishing a BPA under a GSA Schedule, the ordering activity must address the frequency of ordering, invoicing, discounts, requirements (e.g., estimated quantities, work to be performed), delivery locations, and time. For information on establishing a BPA, please refer to https://www.gsa.gov/portal/content/199393.

4.2.7 Using Service Contracts for Cloud Computing Services

Many cloud services requirements can be and should be acquired using the DoD 5000.74 Defense Acquisition of Services 7 step processes. DAU provides Services Acquisition Workshops (SAW)s to assist programs in laying out service contracts. Cloud service considerations per each of the 7 steps are laid out below:

[13] Army ACCENT was issued as a basic ordering agreement (BOA) under FAR 16.7.

Acquisition and Legal	Obtain Leadership Support, Build Team	Analyze Current Acquisition Strategy and Define Objectives	**Support BCA, Alt Analysis, & Cloud Market Research**	Develop Contract Requirements	Develop PWS, QASP, & ACQ Strategy	Select CSP, Negotiate CSP Contract Obtain NDAs	Manage CSP Prepare For Contract End & New Contract
Security	Build Team for Risk Analysis and Security Assessment	**Conduct Cloud Security Risk Assessment Define Cloud Security Training Requirements**	Support BCA, Alt Analysis, & Cloud Market Research	Determine Assess Security Controls Req. & Cert/Test Plan	Support ACQ Strategy Development Complete Assessment Plan & Training	Security Testing & Security Certification ATO	Publish Security Assess and Controls Continuous Monitor/Test
Engineering	Build Team and Start Collecting System Docs	Baseline Current IT Infrastructure & Id Cloud Candidate Systems/Appls	**Support BCA, Alt Analysis, & Cloud Market Research**	Define Eng. Requirements Prepare CS Architecture	Support ACQ Strategy Development Solution Design	Work with CSP to Implement Solution, Test, & Doc Solution	Process Improvement and document CSO
Privacy	Build Privacy Team	Assess Privacy Risk of Candidate Systems & Appls.	Privacy Risk Assessment	Privacy Impact & NARA Assessment	Prepare SORN for Legal Review	Post SORN & Test Privacy Controls	Continuous Monitoring
Project	Develop Initial Project Documents	Complete Project, Coms, & Risk Management Plan	Project Coms, Monitoring and Reporting	Project Coms, Monitoring & Reporting	Project Coms, Monitoring & Reporting	Project Coms, Monitoring & Reporting	Project Closeout
Milestones	Leadership Approval & ID Project Team, Plans & Stakeholders	Baseline Assessment & Project Plans	**BCA, Alt Analysis, & Cloud Market Research**	Approved Requirements & Security, Test, Updated Project Plans	Strategy, Design, & Contracts Approved	Approved CSP Contract, Cloud Service Implemented, SOPs, & NDAs	**Updates to DITPR, FedRAMP, SNAP, and SNaP-IT**

4.2.8 Specific Areas of Concern that Might need Additional Contract Clauses.

Data Jurisdiction

No NIST SP 800-53 controls govern data location; providers may describe boundaries that include foreign data centers. Agencies with specific data location requirements must include contractual requirements identifying where data-at-rest (primary and replicated storage) shall be stored.

- Sample Template Language for Technical Requirements (highlighted items to be filled in by requirement author):

The vendor shall identify all data centers that the data at rest or data backup will reside. All data centers will be guaranteed to reside within (user fill in all yellow highlighted areas:) defined boundary / country / jurisdiction.

The vendor shall provide a Wide Area Network (WAN), with a minimum of # data center facilities at # different geographic locations with at least # Internet Exchange Point (IXP) for each price offering. The vendor shall provide Internet bandwidth at the minimum of # GB.

4.3 Technical Considerations (Engineers/IT Specialists)

4.3.1 Technical Considerations for Cloud Characteristics

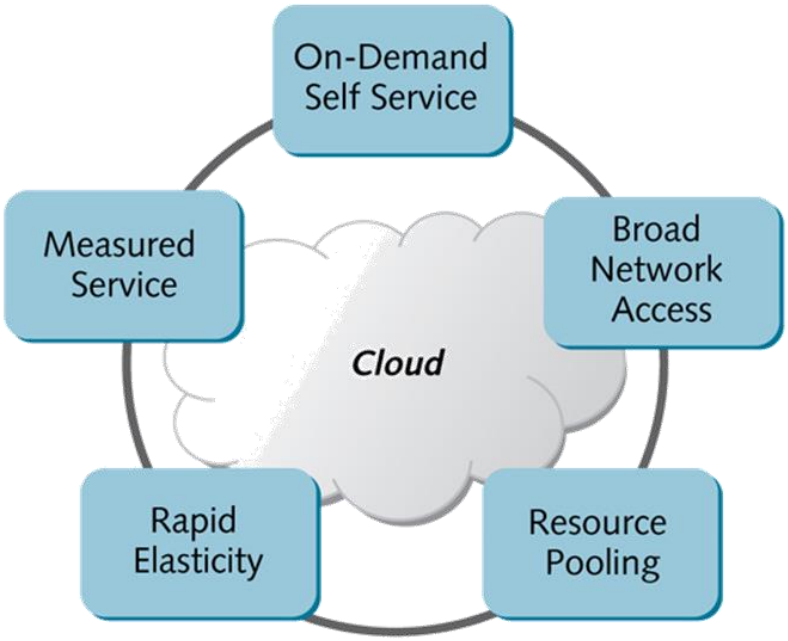


Figure 9. Cloud Characteristics

This section provides a detailed analysis of the five Essential Characteristics of Cloud Computing defined in general terms in Section 2 Foundations of Cloud Computing. The approach is to decompose each characteristic so that technical personnel can determine if a computing capability offered is truly a cloud solution. This information could help in evaluating and differentiating the services among providers during a technical evaluation.

It is important to understand the meaning of the term “essential.” In the context of NIST SP 800-145 and this document, “essential” means each cloud service provider (CSP) **must have the capability to offer and to provide each essential characteristic to the cloud service customer** (CSC) for a given service.

The acquirer may not require each essential characteristic in a specific instance. In addition, the customer must make a subjective judgement to determine if their requirements are fulfilled and to decide if the CSP’s offering can be considered a cloud service for their purposes.

The process of categorizing a computing capability is not always definitive because the requirements for the service will vary by customer. Therefore, this Guidebook allows flexibility in determining that a computing capability qualifies as a cloud service by providing options for evaluating each capability.

Table 11. Overview of the Five Essential Characteristics of Cloud Computing

Cloud Characteristic	Criteria	Options	Notes[14]
On-Demand Self-Service	Computing capability can be provisioned without human interaction with the service provider	• The customer can assess whether the capability is offered **with** fully automated service provisioning (both the customer interface and the internal cloud infrastructure). • The customer uses an automated interface to request and track the service, but the CSP may manually provision the service internally.[15]	"A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider."
Broad Network Access	The computing capability is available from a wide range of locations using standard protocols.	• Available over the Internet • Available over a network from all access points the customer requires	"Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations)."

[14] Peter Mell and Timothy Grance, The National Institute of Standards and Technology (NIST) Definition of Cloud Computing, Version 15, NIST Special Publication 800-145, Sept. 2011, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

[15] Only the CSP can provide verification.

Table 11. Overview of the Five Essential Characteristics of Cloud Computing

Cloud Characteristic	Criteria	Options	Notes[14]
Resource Pooling	The computing infrastructure is shared among more than one consumer.	• Two or more consumers can share the cloud service resources using a multi-tenant model	"The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth."
Rapid Elasticity	The computing capabilities can be "rapidly" provisioned and released to scale.	• Resource allocation modification is automated and near-real-time. • Not fully automated, but fast enough to support the requirements of the customer.	"Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time."

Table 11. Overview of the Five Essential Characteristics of Cloud Computing

Cloud Characteristic	Criteria	Options	Notes[14]
Measured Service	Cloud services characteristics including resource usage are measured with enough detail to support the requirements of the CSC.	• Tracking units of services consumed and associated costs, and tracking resource usage to the application level. • Monitoring, controlling, and reporting, providing transparency for both the CSP and customer of the utilized service.[16]	"Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service."

4.3.2 Technical Considerations for Cloud Service Models

This section supports the categorization of a given cloud service as a software, platform, or

infrastructure service. This guidance for categorizing cloud services supports Requirement #4 of the U.S. Government Cloud Computing Technology Roadmap Volume I (SP 500-293, October 2014), which calls for "*clear and consistently categorized cloud services.*"

The primary determining factors for categorizing a cloud service are:

- The computing capability that is provisioned (software application, platform or infrastructure);
- The primary use of the service, whether it's an end user, developer, or IT operations.

[16] Typically "metering" is done on a pay-per-use or charge-per-use basis, though metering may be used for "showback," as well as chargeback. For example, in a private cloud, metering may be used to show organizational leadership which parts of the organization are consuming what portion of cloud resources.

Table 12. Overview of the Three Cloud Service Models

Cloud Service Model	Criteria	Categories	Notes
Software as a Service (SaaS)	• The service that is provisioned is a software application, described as computer programs designed to permit the user to perform a group of coordinated functions, tasks, or activities. • The primary customers are end users of software applications.	• Custom (e.g. custom applications built or deployed using PaaS) • Off the shelf (e.g. cloud-based email applications)	The capability provided to the CSC is to use the CSP's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g. web-based email), or a program interface. The customer 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.
Platform as a Service (PaaS)	• Deploy customer-created applications to an acquired commercial cloud infrastructure • The service that is provisioned is a software application, described as computer programs designed to permit the user to perform a group of coordinated functions, tasks, or activities. • The primary customers are end users of software applications.	• Application development platforms • Application deployment platforms • Integration platforms	The capability provided to the CSC is to deploy onto the cloud infrastructure CSC-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The CSC 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 configuration settings for the

Table 12. Overview of the Three Cloud Service Models

Cloud Service Model	Criteria	Categories	Notes
			application-hosting environment.[17]
Infrastructure as a Service (IaaS)	• The service that is provisioned is infrastructure. • The primary customers are an IT Operations role creating, installing, monitoring, and managing services and applications deployed in an IaaS cloud.[18] • The term "arbitrary software" in this context means that the customer can deploy and run many types of VM/desktop software.	• Computing resources • Network resources • Storage resources	The capability provided to the CSC to provision processing, storage, networks, and other fundamental computing resources where the CSC can deploy and run arbitrary software, which can include operating systems and applications. The CSC does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

4.3.3 Technical Considerations for Cloud Deployment Models

The following detailed table of cloud deployment models is summarized from information in the NIST Cloud Computing Standards Roadmap[19].

[17] This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources

[18] The infrastructure service may optionally include a pre-installed operating system and other support VM/desktop software and applications, such as webserver.

[19] National Institute of Standards and Technology, U.S. Department of Commerce, Cloud Computing Standards Roadmap, Special Publication 500-291, Version 2, June 18, 2013, https://www.nist.gov/sites/default/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf

Table 13. Overview of the Four Cloud Deployment Models

Cloud Deployment Model	Criteria	Organization	Categories
Private Cloud	Only one organization can use the cloud service and the underlying resources	Model, definition, and associated risks to an organization remains intact, as the cloud resources are provisioned for exclusive use by a single organization comprising multiple business units. In a private cloud model, the organization gets affected in the following ways: • Organization's cloud resources may be owned, managed, and operated by organization, a third party or a combination • May be on or off premises and provides much greater control over data, underlying systems, and applications • Provides an organization greater control over security, assurance over data location, and removal of multiple jurisdiction legal and compliance requirements	• On-site Private Cloud • Outsourced Private Cloud
Community Cloud	A specific community of customers from organizations with shared concerns have exclusive use of the cloud service and the underlying resources	Model, definition, and associated risks to an organization are shared by other organizations, as the cloud resources are provisioned for exclusive use by a specific community of CSCs from organizations that have shared objectives and requirements. In a community cloud model, the organization gets affected in the following ways: • Organization's cloud resources may be operated by one or more of the organizations in the community or a third party • Get the cost benefits of a public cloud while providing heightened privacy, security,	• On-site community cloud • Outsourced private cloud

Table 13. Overview of the Four Cloud Deployment Models

Cloud Deployment Model	Criteria	Organization	Categories
		and regulatory compliance. • A cloud service auditor can conduct independent assessment of cloud services to confirm the scope of the group and confirm that the service and underlying infrastructure are exclusive to the group.	
Public Cloud	Unrelated customers use the shared cloud service and the underlying resources	Public, customer has no control over how resources are provisioned by the CSP. Additional clarification: • While the CSP may limit access to a service, the customer has no control over the set of users accessing the service	Off-premise hosting by CSP
Hybrid Cloud	At least two or more distinct cloud infrastructures are connected together to facilitate hosted data and application portability	The cloud service infrastructure for each set of customers is virtually separated from the other sets of customers/consumers.	Cloud service infrastructure hardware is shared between all sets of consumers

4.3.4 Technical Application Migration Considerations

A common mistake made by IT personnel at this time is to jump into spinning up cloud instances without taking the time to accomplish solid planning. Without proper planning, the cloud will not deliver its full value and will likely extend the time required for successful migration. Cloud migration is not an infrastructure refresh in which hardware/software is being refreshed. It is an application infrastructure redesign that will change the way IT administrators interact with your systems and change how your applications interact with one another and are delivered to your end users.

There are factors that need to be considered when moving applications to a cloud environment. Some are obvious, while others are not. Below are a few guidelines to consider when undertaking application migration to the cloud. For more information on Application Rationalization and migration see See Appendix F References for CIO's Cloud Smart Application Rationalization Playbook.

4.3.4.1 Resource Usage Versus Availability

Since the acquisition paradigm is shifted when acquiring cloud, the organization is no longer purchasing a certain level of capacity or availability. Cloud-computing acquisitions are usage based, so it is important to understand resource usage for the program. Specifically, it's important to review CPU resource patterns to cost-effectively acquire the correct level of availability. Lessons learned show that organizations often overlook log-on storms in virtual desktop infrastructure (VDI) and application publishing services; these will cause user dissatisfaction if not taken into consideration when architecting the environment. Another consideration is when the I/O and throughput for the Cloud Access Point (CAP) connection is to other resources, which may not be located in the same cloud. An example is for instance a system in Azure needing to connect to a DISA mainframe resource via a CAP.

4.3.4.2 Licensing

Is the application licensed per VM, per core, or for total infrastructure footprint? This can have massive cost implications. If the licensing model requires that all available resources be considered even if not allocated to the client, licensing costs will increase if migrated to a public-cloud platform. Similarly, if the application licensing is based per core and the cloud provider does not offer the ability to configure your cloud environment per core, this will have an adverse impact on your licensing cost. Absolutely ensure all Cloud Licensing Fees are known and spelled out in the beginning in the contract (SOO, PWS, SLA).

4.3.4.3 Existing Access Mechanisms

Consider how users currently access their applications and how this will have to change after migration. During planning, it is important to think about the how the expected user experience might be affected and how to best prepare users. Will there be IP addresses or DNS entries that will need to be updated as part of the migration that will affect end users? Is it possible to migrate groups of users at a time, or is a big-bang approach the only feasible option? Will users need to authenticate to connect to the service, or will they leverage a WAN or MPLS network? Ensure you plan not only for end users, but for developers as well. Can their development application be on their local machine? Does there need to be a VDI in the environment? Does a new VPN need to be created with their own set of accesses? Figure out in the beginning what your requirements are for access.

4.3.4.4 Security

Along with networking, organizations need to carefully look at the implementation of security policies to ensure that the required level of security is adequately met. Certain concessions may be required to relax policies or cede responsibility for particular areas to the cloud-service provider. Alternatively, workarounds can include integration of virtual or physical appliances that complement the cloud architecture and meet compliance demands.

4.3.4.5 Testing

Many unexpected application migration and implementation hurdles can be overcome by a rigorous test strategy. A common misunderstanding with programs moving applications to the cloud is that little or no testing is needed depending on the service model selected (IaaS, PaaS, SaaS). Yet many data breaches are attributed to the customer application and misconfiguration of cloud administration items used for provisioning cloud services to users. A test program will reveal how the application will be managed in the chosen cloud service model and help system managers discover gaps in the administrative processes and misconfigured application

settings.

To facilitate security testing, the contract should address items such as CSP support to government testing and access to test results if previous CSO testing has been performed. Examples of items to consider when developing the RFP, contract, and SLA to facilitate CSP support to DoD T&E and problem resolution:

- Integrate the CSO test environment with representative DoDIN integration points and services to create a representative test environment.
- Engage CSP support to DoD T&E of external functions, interfaces, and integration points to include the DoDIN integration points and services.
- Provide DoD oversight of cybersecurity testing in the CSO environment, such as in a IaaS or PaaS CSO where other DoD programs are being implemented or developed.
- Perform DoD evaluation of CSP, CSSP and operations and support (O&S) in execution of the shared responsibilities.
- Grant DoD physical and logical access to the CSO to conduct DoD cybersecurity T&E and Persistent Cyberspace Operations.
- Ensure DoD access to CSP technical support and documentation for DoD cybersecurity T&E activities, including Mission-Based Cyber Risk Assessments such as Cyber Table Top (CTT) exercises.
- Confirm DoD access to system logs, packet capture, and other CSO information to support problem resolution, test results, and test reporting.
- Enable DoD access to all FedRAMP+ and/or DoD PA-related artifacts (e.g., Security Assessment Report).

For more information about cloud cybersecurity T&E, refer to the DOD Cybersecurity T&E Guidebook v2, April 2018; Addendum: Cybersecurity T&E of DoD Systems Hosted on Commercial Cloud Service Offerings.

4.3.4.5 IT Service Management (ITSM)

Maintenance and change window procedures, service desk alignment, and a general review of ITSM processes ensure that while more elements of the environment are outsourced, policies and processes align to the requirements of the organization. Finger pointing when things go wrong is a consequence of unclear expectations.

4.3.4.6 Integration

Organizations often discover application dependencies too late in the process of migrating workloads, resulting in unplanned outages and limited functionality to systems while these dependencies are addressed. Understanding the relationships between applications is critical to planning the sequence and manner in which cloud migrations occur. Can the application exist on the cloud in isolation while other systems are migrated?

4.3.4.7 Replication

Data protection requirements, the manner and the frequency in which replication occurs, and aligning the recovery time objective (RTO) and recovery point objective (RPO) of applications to their business criticality

influence architectural designs. Source the appropriate solutions to provide the necessary levels of data transfer in terms of capacity and costs. Ensure you understand enclave isolation and the possibility that the resource cannot be replicated.

4.3.4.8 Application Architecture

Organizations should review each application architecture not only for a compatibility view, but to support optimization of the cloud platform. Monolithic systems make it difficult to scale efficiently and respond quickly, thereby removing the cloud's agility benefits. It is absolutely critical to review the application architecture in order to ensure that migration of these applications to a cloud environment is the right decision.

Moving production applications to the cloud requires careful thought and an openness to the re-architecture of not only the application space, but surrounding processes and policies. Various providers may recommend a cloud-only approach, but this may not always be the best solution for all your applications. A careful design that accounts for all IT environment factors and business outcomes may instead yield a hybrid solution.

Many businesses are finding that an infrastructure that delivers cloud at the core but is flexible to continue to cater for some workloads on physical infrastructure is the best solution.

4.3.5 SCCA DISA's Secure Cloud Computing Architecture (SCCA)

SCCA is a suite of enterprise-level cloud security and management services. It provides a standard approach for boundary and application level security for impact level four and five data hosted in commercial cloud environments.

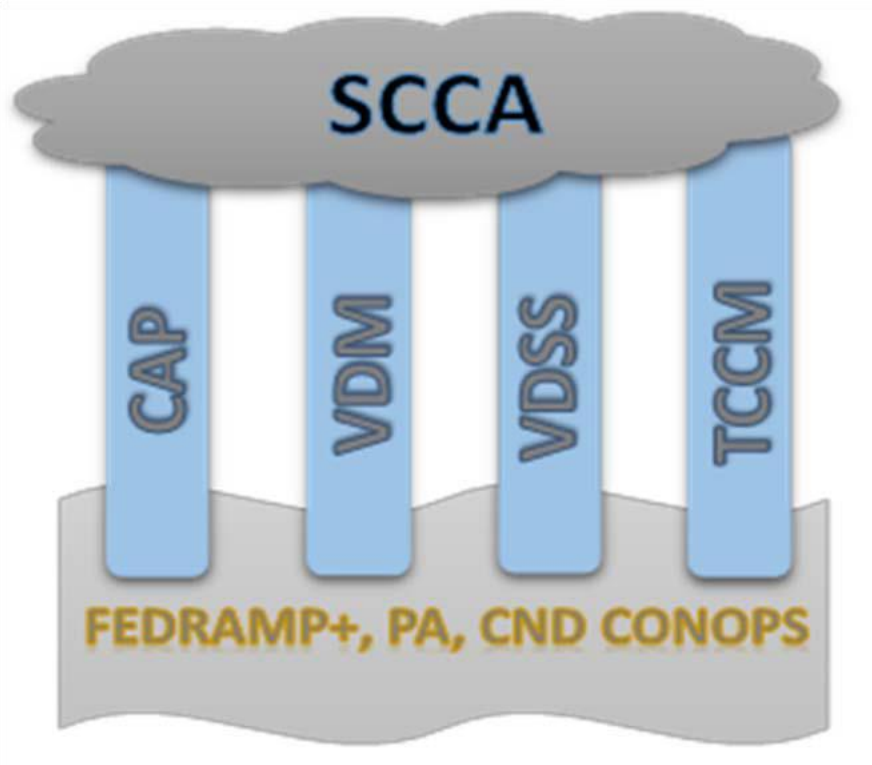


Figure 10. Secure Cloud Computing Architecture (SCCA)

Features include:

- Cloud Access Point (CAP): Provides access to the cloud and protects DOD networks from the cloud. Streamlined protections focused on protecting the network boundary.
- Virtual Data Center Security Stack (VDSS): Virtual network enclave security to protect applications and data in commercial cloud offerings.
- Virtual Data Center Managed Services (VDM): Application host security for privileged user access in commercial environments.
- Trusted Cloud Credential Manager (TCCM): Cloud credential manager to enforce role-based access control (RBAC) and least privileged access.
- Connect: Access DoD approved level 4/5 cloud service providers.
- Secure: Extend application and data-level security services to the cloud.
- Manage: Obtain custom analytics and intelligence data for host-based security and role based access controls.
- Boundary Defense: Connect to approved Level 4/5 providers and protect providers and protect
- DoD networks.
- Web Application Firewalls: Prevent targeted attacks; cross-site scripting, forceful browsing, cookie poisoning, and invalid input.
- Next Generation Firewalls: Virtual appliance architected to identify network traffic and implement policies in a mission-centric fashion.
- Host Based Security Service: Develop cloud-based orchestration for security policies, upgrades, and reporting.
- Assured Compliance Assessment Solution: Manage roles, scan zones, and policies.
- System Patching: Cloud-based DoD patch repositories.
- Recursive DNS Caching: Forward and cache external DNS queries.

SCCA Scope and Capabilities. The SCCA is designed to cover all aspects of commercial provider implementation. It addresses the security concerns inherent in today's industry offerings for infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS). Additionally, it includes support for both on premise and off premise commercial providers.

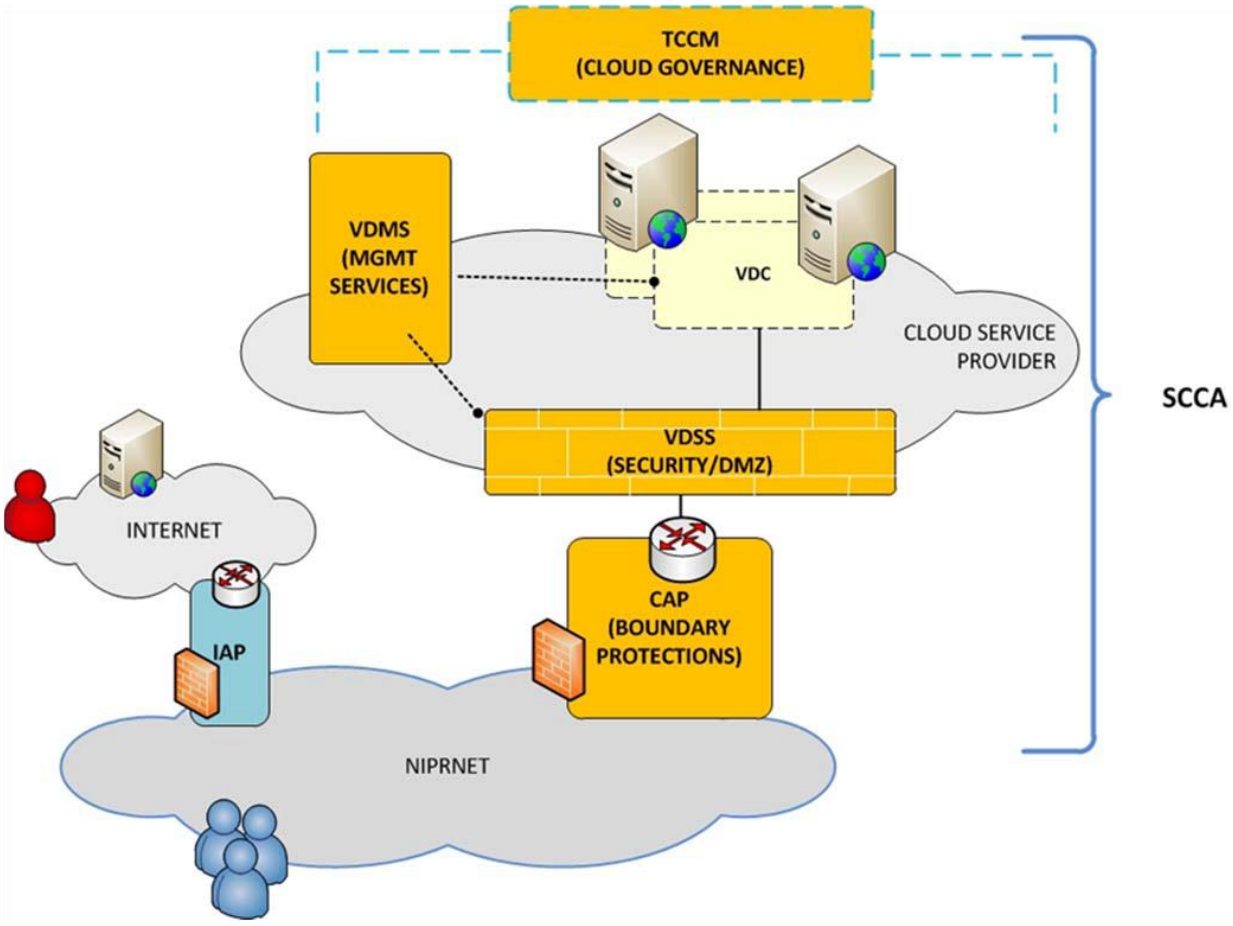


Figure 11. SCCA Boundary CAP (BCAP)

BCAPs Do Not Break and inspect and Do Not Provide application level security.

4.3.6 Emerging Cloud Technology

It is important for technical personnel assigned to Cloud acquisition programs to understand the rapidly emerging technology areas for cloud computing. This will help when evaluating technical proposals from CSPs.

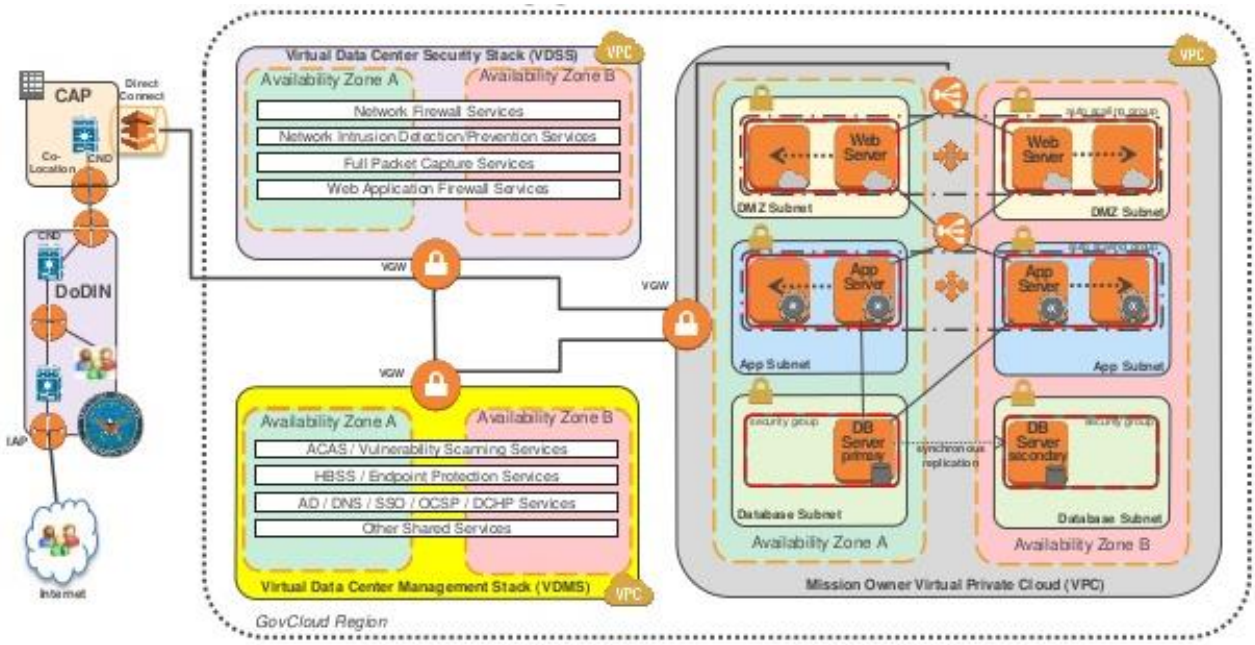


Figure 12. SCCA Architecture Approach in AWS

4.3.6.1 Containers and Microservices

More and more, organizations are using containers and microservices to spur digital growth as the next step from the virtual machine environment.

A trend since the early 2000's in data centers used for in-house enterprise applications and cloud computing services is the increasing adoption of Hardware or Server Virtualization. Hardware virtualization enables running multiple computing stacks called System Virtual Machines (S-VMs) on a single physical host. An S-VM in the context of hardware virtualization is made up of a complete computing stack (or engine) consisting of one or more applications, Operating System (called the Guest OS) and virtual hardware. S-VMs are able to perform their tasks due to an intervening hardware emulation layer or hypervisor that runs between the S-VMs and the hardware of the physical host.

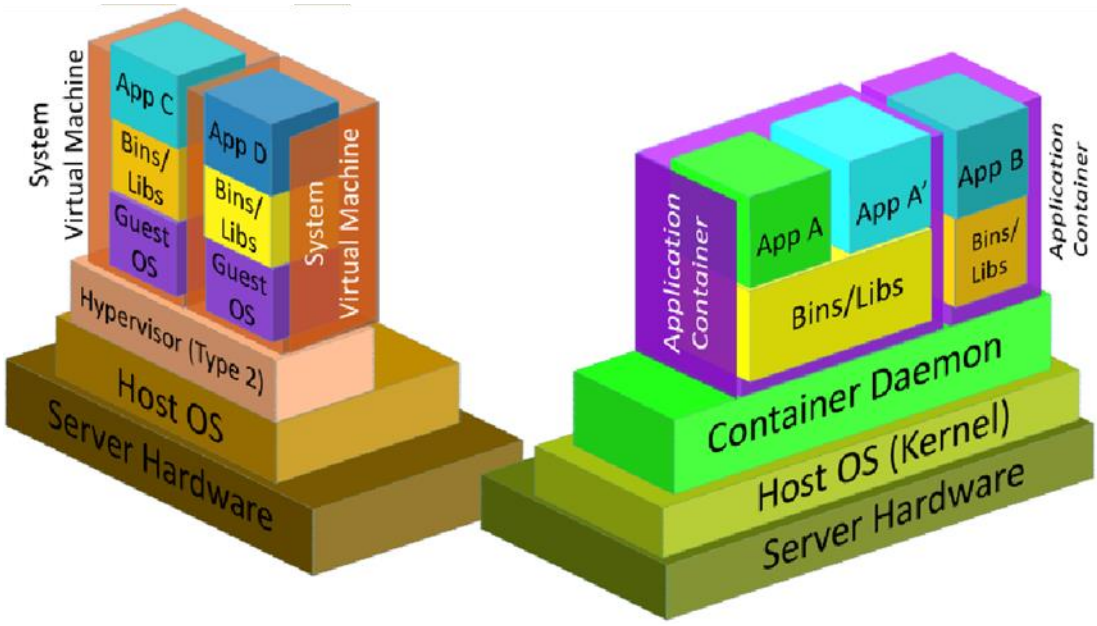
Another trend is to virtualize applications at the OS layer. Just like multiple S-VMs run on the same physical hardware, in this context, multiple instances of an entity called "Application Containers" run on top of an OS's kernel in user space. Just like hardware virtualization allows multiple OS instances to run on a single physical host, application container technology allows multiple isolated user space instances (processes) to be run on a single host. Application containers are made of up application code (e.g., webserver or DBMS server) which has access to a collection of libraries/binaries that represent an OS's core capabilities. Each library component provides a traditional OS function such as memory, namespace and processes needed for that application code to work. The application container, when deployed, provides an execution environment for applications in the form of isolated processes.

Application components that are placed into a container can leverage a Microservices architecture. A Microservices architecture can be contrasted with a Service-oriented architecture (SOA) wherein Microservices

consist of small, stateless, loosely coupled and isolated processes built around capabilities as opposed to services. Microservices are independently deployable in Application Containers, use less resources and can be created, destroyed, started and stopped far faster than in a SOA.

Definitions:

- **Microservices**: A microservice is a basic element that results from the architectural decomposition of an application's components into loosely coupled patterns consisting of self- contained services that communicate with each other using a standard communications protocol and a set of well-defined APIs, independent of any vendor, product or technology. Microservices are built around capabilities as opposed to services, builds on SOA and is implemented using Agile techniques. Microservices are typically deployed inside Application Containers.
- **Application Containers**: An Application Container is a construct designed to package and run an application or its' components running on a shared Operating System. Application Containers are isolated from other Application Containers and share the resources of the underlying Operating System, allowing for efficient restart, scale-up or scale-out of applications across clouds. Application Containers typically contain Microservices.
- **System Virtual Machines**: A System Virtual Machine (S-VM) is a software implementation of a complete system platform that supports the execution of a complete operating system and corresponding applications in a cloud. Each S-VM serves as an efficient, isolated duplicate of a real machine running on a cluster of physical machines. Differences in S-VMs and Application Containers. S-VMs abstract the Operating System from the underlying hardware, allowing for multiple Operating Systems and Application to share a single system's physical compute resources. Application Containers abstract the Application from the underlying Operating System, allowing for multiple Applications to share a single system's Operating System and underlying physical compute resources[20]



[20] DAU ISA 101 on-line course, Lesson 20 Cloud Computing.

Figure 13. Differences between S-VMs and Application Containers

DevSecOps Paradigm: As an integral part of their digital roadmap, many organizations are embracing agile development frameworks to gain time-to-market by combining development, quality assurance and operations tasks. This new paradigm leverages continuous integration and continuous development (CI/CD) methodologies and breaks down silos to automate software testing and security, streamline processes and enforce close interaction. A container includes a complete file system that encompasses the code, runtime, system tools and libraries – in other words, all components an application needs to run. This not only makes code more portable, but also makes applications more resilient and allows for rapid deployment.

- **Microservices:** Microservices are gaining traction because they enable developers to isolate functions easily, which saves time and effort, and increases overall productivity. Unlike monolith applications where even the tiniest change involves building and deploying the whole application, each microservice deals with just one concern.
- **Capacity management:** Memory plays a crucial role when it comes to containers. Cluster managers look at the total memory capacity available on the host compared to the memory requested by containers to determine on which host to deploy it. In case of insufficient free capacity, a container will not be deployed. Typically, each container runs in a single encapsulated process with shared infrastructure underneath. With their own operating environment attached, images can easily reach a couple of hundred megabytes in size. Thus, lifecycle management – especially retiring old images – requires constant attention to free up shared resources and avoid capacity constraints.
- **Network Layer:** Other potential bottlenecks can be the network used within the cluster and the network virtualization layer used to connect containers across multiple clusters, which requires close monitoring in terms of performance, load balancing, and seamless interaction between the two. Moving forward, the necessity will further increase when keeping in mind that one out of five respondents will be having over 50 percent of their apps in the cloud by end of 2017, as recently reported by F5 Networks. This is even more important when operating at scale in a hybrid scenario or a multi-cloud environment comprising shiploads of containers spread across multiple service providers.
- **Lifecycle Management and Orchestration**: Both containers and microservices can easily be replaced and therefore tend to have a relatively short lifespan. Organizations employing container orchestration frameworks to automate the start and stop of containers achieve higher churn rates. The short lifespan combined with the enormous density lead to an unprecedented number of items that require monitoring.
- **Monitoring**: Many traditional IT monitoring tools don't provide visibility into the containers that make up those microservices, leading to a gap somewhere between hosts and applications that is ultimately off the radar. As soon as the attached applications go live, IT operations teams could suddenly find themselves either blind or flooded with a tsunami of alerts. Neither extreme is good. Inconsistent and fragmented alerts could occupy huge amounts of resources in avoidable troubleshooting. Despite all the enthusiasm around microservices and cloud-native applications, legacy applications won't disappear anytime soon. Thus, organizations need to put one common monitoring in place comprising both worlds and covering the entire IT stack – from the bottom to the top.
- **Manageability:** Organizations need to ensure that they have allocated sufficient manpower to manage an exponentially growing estate of microservices. Not only will all the APIs that the containers need to invoke require continuous housekeeping, but once employed, microservices have a strong tendency to multiply unless managed diligently. All too often, developers are tempted to add new functionality by creating yet another microservice. In no time, organizations find themselves attempting to manage an army of containers and countless microservices competing for the same IT infrastructure underneath. Organizations must therefore employ analytics tools that discover duplicative services and detect patterns in container be-havior and consumption to prioritize access to systems resources.
- **Container Orchestration:** The industry is now moving forward from managing one container on one host to managing multiple containers deployed on multiple hosts. To go beyond the management of individual containers, the next step is container orchestration. Orchestration tools extend lifecycle

management capabilities to complex, multi-container workloads deployed on a cluster of machines. By abstracting the host infrastructure, orchestration tools allow users to treat the entire cluster as a single deployment target. There are tools and methods available to accomplish these tasks. Among these are Docker Swarm, Google's Kubernetes, and an open source cluster manager called Apache Mesos.

4.3.6.2 Conclusion

Organizations are under pressure to create more agile IT environments that support their organization's digital business strategies. Containers and microservices will play an important role in accomplishing these objectives by enabling the organization to accelerate release cycles and gain efficiency.

In theory, microservices are designed to make managing IT easier. However, without solid planning and continuous housekeeping, organizations might be overwhelmed and soon find themselves confronted with exacerbating long-standing issues rather than solving them. In fact, it takes time and effort to operate containers and microservices at enterprise-grade. Both natively offer only limited visibility, which can be painful when it comes to processes that are business critical. Not being able to fix or even detect the problem due to missing visibility into the application landscape is an area of risk that would need to be managed.

4.3.7 Technical Considerations with CSPs

The following technical considerations need to be examined for each Cloud acquisition. The DoD organization must understand how the CSP addresses the following:

4.3.7.1 Application and Service Portability

How is this done? Are there proprietary encryption or compression routines that make it difficult for the customer to migrate from cloud service provider to another or back to in-house?

- **Isolation Failure:** For example, how does the vendor isolate data/traffic? There is risk of failure if the service provider does not have solid mechanisms that separate storage, memory, and routing.
- **Management Interface Compromise:** Management interfaces of public clouds are often Internet accessible and pose additional risk when combined with remote access and browser vulnerabilities. How does the CSP manage their interfaces?
- **Data Protection:** The customer has no real insight into the CSPs data handling practices. Some of the data protection risk is mitigated by FedRamp+ and DoD Cybersecurity architectures and requirements. However, it would be good to know what level/type of access CSP personnel have to DoD Data.
- **Insecure or Incomplete Data Deletion:** In the case of multiple tenancies and the reuse of hardware resources there is a risk of untimely or inadequate data destruction. Ask the CSP how they handle data deletion.

4.4 Cybersecurity Considerations

Probably the most important Cybersecurity fact is for DoD acquisition professionals to clearly understand that (Cyber) Security in the Cloud is a ***shared responsibility*** between the cloud service provider and the mission owner. It is critical to know and understand who is responsible for accomplishing all required activities and artifacts before trying to put a requirement on contract. This section should assist in understanding how to accomplish this.

Another key fact to understand is that even if the Cloud Service Provider owns the facilities and associated infrastructure, it is still true that only a DoD Authorizing Official has the authority to provide an Authorization to Operate (ATO). For specific considerations for cybersecurity in an SLA or contract, reference the Cybersecurity table in Appendix B: Example SLA Checklist.

4.4.1 FedRAMP and Provisional Authority to ATO (P-ATO)

In Section 3 DoD Approach for Acquisition of Commercial Cloud Services, information was provided to describe the first steps in the cybersecurity path for a CSP to be able to provide infrastructure services. The foundation for the CSP to be able to provide CSOs to DoD programs is to obtain a Provisional Authority (PA) from the Joint Authorization Board (JAB). This essentially verifies that the CSP has met the required NIST controls. The topics in this section assume that those activities have already been accomplished and that a PMO is competing their requirements within a pool of authorized vendors for their data impact level IAW the DoD SRG CC.

In December of 2011, the Federal Chief Information Officer released a new policy, Security Authorization of Information Systems in Cloud Computing Environments, detailing the new Federal Risk and Authorization Management Program (FedRAMP). As of June 2016, FedRAMP program provides is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a “do once, use many times” framework that saves an estimated 30-40% of government costs, as well as both time and staff required to conduct redundant agency security assessments. FedRAMP is the result of close collaboration with cybersecurity and cloud experts from the General Services Administration (GSA), National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Department of Defense (DOD), National Security Agency (NSA), Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) Council and its working groups, as well as private industry.

The DoD added additional controls to FedRamp for DoD authorizations via FedRamp+. For DoD CSOs, Joint Authorization Board (JAB) Provisional-ATOs are needed and issued via a prioritization process in which a business case is submitted to the FedRAMP program office. The business case is reviewed and examined against the current criteria, and if selected, the cloud solution is reviewed and authorized via the JAB. **The authorization package is then made available for review by the acquiring agency**. JAB authorizations are only granted on the CSPs environment and contain a Customer Responsibility Matrix (CRM). The CRM contains the controls that are shared by, or the responsibility of, the acquiring agency. The JAB ATO should be leveraged by an agency and be included in an agency’s overall ATO package. Agency use of any services outside of the scope of the leveraged ATO will require their security evaluation and assumption of the associated additional risk. This requires vigilance for security on the part of acquiring organizations to the services and solutions

deployed.

It is important to note that the authorization package should be reviewed by the acquiring agency before a decision to acquire the cloud solution is made since each FedRAMP ATO covers only a particular cloud service offering (CSO) of the CSP of which they may have several. **CSP's with several cloud service offerings will have separate FedRAMP ATO's for each offering.** The scope of each ATO is defined by the security boundary established within the particular solution covered and, more importantly, may not cover all services marketed by the CSP as being part of the offering.

4.4.2 Recommended Cybersecurity Policies for Contracts

This section outlines best practices for including cloud cybersecurity requirements in DoD contracts. There are many types of contracting approaches in the DoD. For many cloud acquirers, the contract type is an Indefinite Delivery/Indefinite Quantity (ID/IQ) type of base contract. Most program offices write task orders or delivery orders for their specific requirements. If using a Task Order or Delivery order under an IDIQ contract, first check to see if the cloud cybersecurity polices listed below are on the overarching contract as a compliance requirement. If so, the Program Management Office (PMO) may not need to also put these requirements on individual Task Orders or Delivery Orders. Check with your contracting officer. Some IDIQ contracts list policies and standards and say, "If applicable for individual Task Orders". If this is the case, you would then list the applicable policies and standards on your task order or delivery order. However, when put on any contract, a best practice is to add the verbiage "or current version" to the policy referenced so that the requirements reflect any updates to policy. Recommended cloud cybersecurity policies and best practices include:

- Acquired CSP infrastructure connected to the Department of Defense Information Network (DoDIN) is subject to DoDIN security requirements and standards (Reference
- Joint Publication (JP) 3-12 (R): Cyberspace Operations, dated February 5, 2013)
- Classified Contractor infrastructure must follow the National Industrial Security Program as established by Executive Order 12829. (Reference Executive Order 12829 - National Industrial Security Program, dated January 8, 1993)
- The DoD Cloud Computing Security Requirements Guide (DoD CC SRG) establishes core requirements (Reference DoD Cloud Computing Security Requirements Guide, Version 1 Revision 3 dated March 6, 2017).
- Contractor must provide the ability for actions to be logged to an immutable destination within the cloud offering. Such logs must provide an audit trail that supports the functions outlined in DoD Instruction 8530.01. (Reference DoD Instruction 8530.0l: Cybersecurity Activities Support to DoD Information Network Operations, dated July 25, 2017).
- Cyber incidents and breaches must be reported in accordance with DFARS 252.239-7010.
- The DoD operators and/or auditors are authorized to verify compliance with standards and policies to include FedRAMP, the DoD CC SRG, and other applicable policies.
- Infrastructure must be accredited in accordance with the applicable DD Form 254 on the contract/task order/delivery order.
- Classified and unclassified server and media destruction is to be pursuant to DoD Directive 5220.22-M. (Reference DoD Directive 5220.22-M: National Industrial Security Program Operating Manual, dated February 28, 2006).
- Physical isolation must be compliant with National Security Telecommunications and Information Systems Security Advisory Memoranda (NSTISSAM) Level. (Reference National Security Telecommunications and Information Systems Security Advisory Memoranda (NSTISSAM) Level I: Compromising Emanations Laboratory Test Standard)
- Logical separation of unclassified infrastructure and encryption with FIPS 140-2 approved cryptographic

implementations is required for data both at rest and in transit. Encryption pursuant to CNSSP 15 is required for unclassified NSS data both at rest and in transit. (Reference National Security Telecommunications and Information Systems Security Advisory Memoranda (NSTISSAM) Level I: Compromising Emanations Laboratory Test Standard)

- Logical separation within classified infrastructure requires encryption with NSA approved cryptography for data both at rest and in transit pursuant to CNSSP15. (Reference Committee on National Security Systems (CNSS) Policy 15: Use of Public Standards for Secure Information Sharing, dated October 20, 2016).
- Contractor must support management of encryption keys internally and by the government pursuant to CNSSP 30. (Reference D.13 CNSS Policy 30: Cryptographic Key Protection, dated December 28, 2017.)
- Unclassified authentication requires MFA such as DoD PKI as defined in DoD Instruction 8520.03. (Reference DoD Instruction 8520.03: Identity Authentication for Information Systems, dated July 27, 2017 and subsequent guidance dated June 2018).
- Access to classified infrastructure requires DoD PKI-based authentication at the appropriate classification level pursuant to DoD Instruction 8520.03 and CNSSP 25. (Reference DoD Instruction 8520.03: Identity Authentication for Information Systems, dated July 27, 2017 and CNSSP 25: National Policy for Public Key Infrastructure in National Security Systems, dated December 11, 2017).
- Highly granular access control configuration is required for compliance with technical policies as defined in NIST SP 800-63. (Reference NIST SP 800-63: Digital Identity Guidelines, Revision 3 dated June 2017).
- Secure data transfer capabilities provided must meet DoD's requirements as described in the 2018 Raise the Bar Cross Domain Solution Design and Implementation Requirements document. The secure data transfer capabilities will be assessed in accordance with DoD Instruction 8540.01 and CNSSI 1253F Attachment 3, Cross Domain Solution (CDS) Overlay, September 2013.
- Classified and unclassified server and media deletion is to be pursuant to NIST SP 800-88 (0 .17].
- Account management, authentication, and authorization services must be isolated from those used by other customers; ability to prevent access to these services from the Internet and any other network not specifically authorized.
- For traffic of data above IIL Level 2 moving between the DoDIN and any Contractor Point of Presence (POP) that bypasses DoD's Cloud Access Point (CAP) requires approval of the DoD CIO or their designated representative(s).[21]
- The CSP must support both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) network addressing.22 IPv6 is the Internet Protocol for carrying data “packets” from a source to a destination over a number of networks. IPv6 is the enhanced version of IPv4, supporting a larger number of nodes or communication endpoints. DoD is committed to implement IPv6 because IPv4 cannot support future required combat systems and is currently preparing for eventual IPv6 migration.
- The CSP and PMO will coordinate forensic and compliance audits pursuant to NISTIR 8006l0. (Reference NISTIR 8006: Cloud Computing Forensic Science Challenges, dated June 30, 2014)
- Records must be available to the CCPM in accordance with the Federal Records Act (Reference U.S. Code Chapter 31: Records Management by Federal Agencies)
- The Contractor is to support DoD's role in providing Cybersecurity Support services in accordance with the DoD CIO Cybersecurity Service Provider Memorandum. (Reference DoD Memorandum: Cybersecurity Activities Performed for Cloud Service Offerings, dated November 15, 2017).

---

[21] Department of Defense, Cloud Computing Security Requirements Guide, March 6, 2017, https://iasecontent.disa.mil/cloud/Downloads/Cloud_Computing_SRG_v1r3.pdf.

[22] https://www.nitrd.gov/subcommittee/lsn/jet/presentations/R%20Broersma_DoD%20IPv6%20Briefing%20for%20DREN.pdf

http://www.usipv6.com/ppt/IPv6SummitPresentationFinalCaptDixon.pdf

- Ensure unauthorized access does not occur. (References: CNSS Instruction 1253F Attachment 5: Classified Information Overlay , dated May 9, 2014, DoD Directive 8100.02: Use of Commercial Wireless Devices, Services and Technologies in the Department of Defense Global Information Grid, dated April 23, 2007, FIPS PUB 140-2 : Security Requirements for Cryptographic Modules, dated December 3, 2002, 0MB Circular No. A-130: Managing Information as a Strategic Resource, dated July 28, 2016, CNSS Policy 11: Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products, dated June 1, 2013.
- Provide CSP support to government cybersecurity T&E including access to system logs, packet capture, and other CSO information to support problem resolution, test results, and test reporting. (Reference: DOD Cybersecurity T&E Guidebook v2, April 2018; Addendum: Cybersecurity T&E of DoD Systems Hosted on Commercial Cloud Service Offerings).
- Provide a testing environment that emulates the operational environment to support test and evaluation and the ability to connect a DoD cyber test range emulation of DoDIN infrastructure to the test environment.

Cloud policies that are not cybersecurity specific are found in Appendix F: References.

4.4.3 Cloud Cybersecurity Focus Areas[23]

4.4.3.1 Identity and Access Management (IdAM) Considerations

Support for Common Access Card (CAC) authentication or other high assurance authentication methods is limited, therefore, we offer the following IdAM standards and examples that can be used:

- Federated IDs. The use of IDs that are held directly by the customer or by a trusted third party provider, so that the customer is not obliged to establish and administer an additional set of user identities in order to use each cloud service.
- Single sign-on: Closely allied to federated IDs is the concept of users having a single ID and a single sign-on when using a set of different services, possibly spanning the customer's systems and multiple providers' cloud services.
- Privileged Identity Management: The IDs of cloud service administrators are privileged in their capabilities and need special control. Common identity access management frameworks do not manage or control privileged identities and so specialized privileged identity management is needed. This capability can be used as an information security and governance tool to help customers in meeting compliance requirements and to prevent data breaches through the use of privileged accounts.
- A number of standards and technologies are available which provide federated IDs and single sign-on, including:
    - The Lightweight Directory Access Protocol (LDAP) is an IETF standard widely used to provide access to directory servers, which includes authentication and authorization services.
    - The Security Assertion Markup Language (SAML) is an XML based OASIS standard used for the exchange of authentication and authorization data between security domains – in particular between an identity provider and a service provider.
    - OAuth 2.0 is an IETF standard for authorization. It provides authorization flows for web applications, desktop applications, mobile phones, and intelligent devices, which can be used for cloud services.
    - WS-Federation is an OASIS standard for identity federation in relation to web services. It is part of the wider WS-Security standard and in particular utilizes the WS-Trust standard for the exchange of various tokens.
    - OpenID Connect is a specification that provides an API-friendly layer on top of the OAuth 2.0

[23] DISA Cloud Symposium, 2018, © 2016 Cloud Standards Customer Council, Page 15

protocol.

- The System for Cross-domain Identity Management (SCIM) is an IETF standard for managing user identities across domains – and specifically aimed at the needs of cloud services.
- Active Directory Federated Services (ADFS2) is a proprietary specification from Microsoft supporting single sign-on that is used by many organizations.
- For access control and security policy decisions and enforcement there is:
- The eXtensible Access Control Markup Language (XACML) defines a declarative access control policy language implemented in XML and a processing model describing how to evaluate authorization requests according to the rules defined in policies.
- In addition, digital certificates are an important aspect of IAM, in support of public key infrastructure (PKI) and the establishment of trust when using cloud services. Cloud service customers should be aware of the support that the cloud service provider has for digital certificates, including PKCS, X.509 and OpenPGP.
- Access control determines what type of authorizations should be provided to cloud accessible resources by the cloud service provider for authenticated users. Customers should require fine-grained access control both for stored data and for applications, to enable the customer to enforce their security policies. The aim should be to have access control granularity at least equivalent to that used for customer in-house systems. This includes being able to create and manage authorization policies.

Figure 14 depicts an example Cloud architecture for Identity and Access.

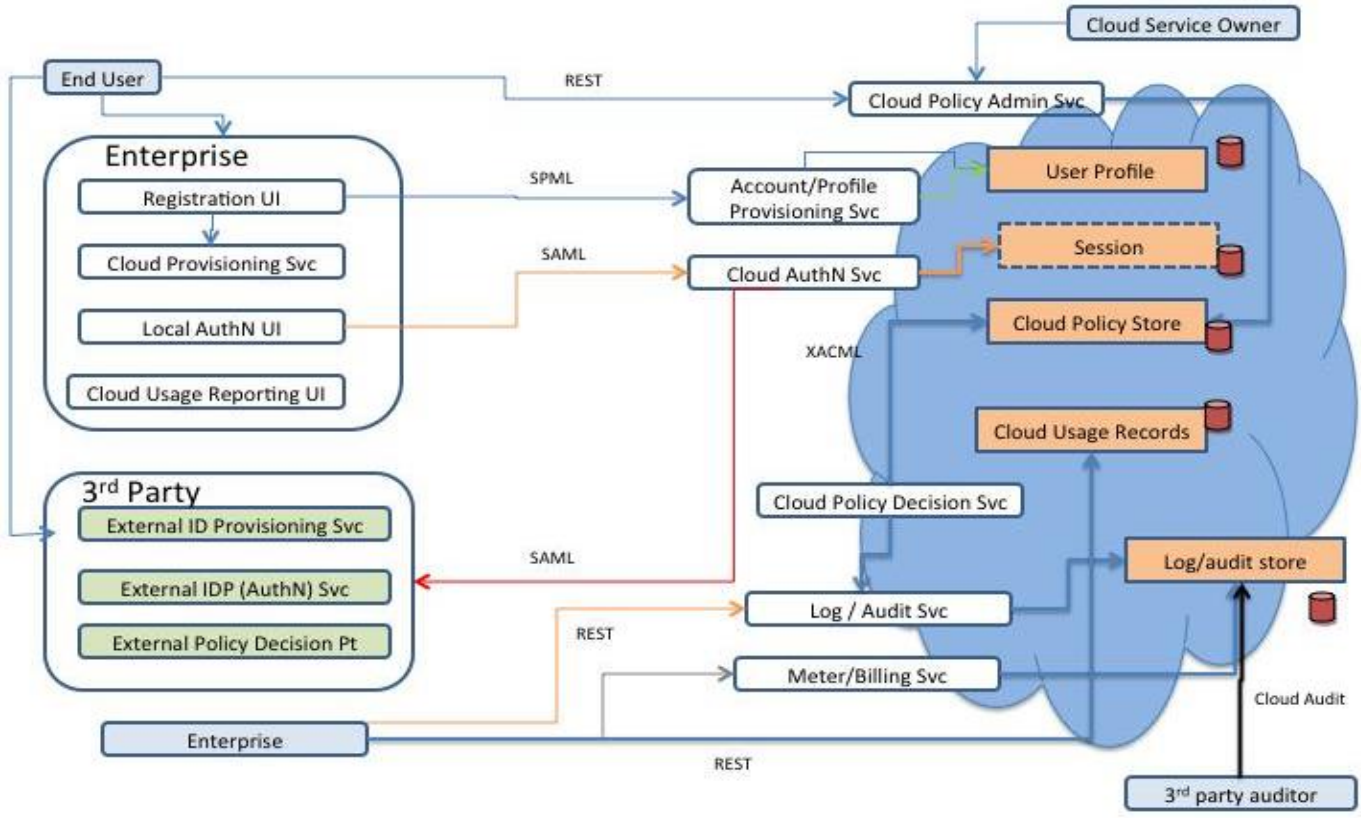


Figure 14. Cloud Identity/Access Architecture Pattern

4.4.3.2 Protecting DoD Data in the Cloud

- The Department's ability to protect its data and respond to cyber incidents is maturing
- DoD working with the CSPs to deploy new tools and techniques to enhance capabilities (e.g. Secure Cloud Computing Architecture)
- CSSP Services to support defense of systems and data in the Cloud

To ensure data is protected in DoD cloud deployments, programs should consider the following test items:

- Verify mechanisms to ensure Government data is protected from unauthorized disclosure and remains under government control
- Verify configuration and protections of external and internal data flows between applications, containers, virtual devices, VMs, CSO infrastructure, and DoD Infrastructure
- Verify data at rest encryption on CSP infrastructure
- Verify data leak protection between applications, virtual machines, or physical infrastructure

4.4.3.3 Secure Connections to the Cloud

- Communications with mission critical off-premise cloud providers requires reliable and appropriately secure with capacity to support mission needs
- Use the new generation of the DoD (DISA) Cloud Access Point(s) CAP
- DoD is working with Industry on other potential approaches for commercial CSP connectivity

Table 14. Non-DISA Provided DoD Cloud CAPS, August 30, 2018

CAP	Approved	Date	Notes
USMC	Yes	4/30/2018	Valid for 180 days, pending assessment
DHA (Med-COI)	Yes	12/27/2017	Pending assessment
Navy SPAWAR	Yes	4/30/2018	Approved
DREN	No		Pending technical review, waiting on DREN
CTTSO (SUNet)	Yes	11/20/2017	Pending assessment
JSP	No		No formal application submitted
APAN	No		Assessment should be complete by June 30.

4.4.3.4 Cybersecurity Assessments

The growing number of CSPs and CSOs create an assessment challenge and FedRAMP and 3PAOs should be leveraged to support the assessment process. The use of an approved CSP does not relieve the program of their obligations to thoroughly understand and test the shared responsibilities (e.g., what the CSP responsible is for and what the government responsible for from an operational security standpoint). For more information about cloud cybersecurity assessments, refer to the DOD Cybersecurity T&E Guidebook v2, April 2018; Addendum: Cybersecurity T&E of DoD Systems Hosted on Commercial Cloud Service Offerings.

The following process will outline how CSPs and CSOs are assessed.

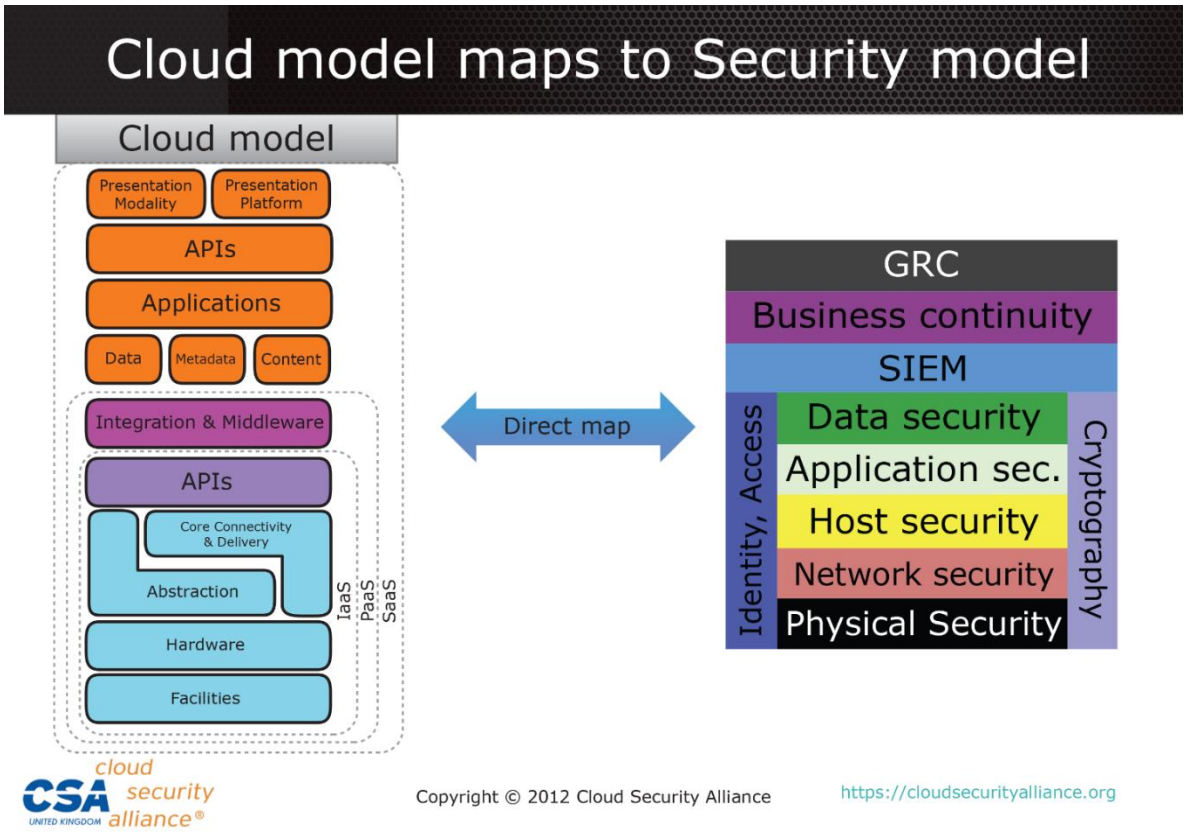


Figure 15. Cloud Model Maps to Security Model

4.4.4 FedRAMP and ISO 27001 Certification Considerations[24]

As mentioned in Section 3 DoD Approach for Acquisition of Commercial Cloud Services and above, FedRAMP was introduced to provide a cost-effective, risk-based approach for the adoption and use of cloud services in the federal government. The idea was to define a set of standardized security requirements for the authorization and ongoing cybersecurity of cloud services based on different system impact levels (risks) and a "certification program" supported by a large team of FedRAMP authorized independent, third-party assessment firms. Theoretically, at that point, the security experts from the DHS, DOD, and GSA could maintain a list of "approved" Cloud Service Providers.

There are a few things to understand about FedRAMP:

- For most CSP attempting to become FedRAMP compliant, it may take up to 15 months post proclamation.

[24] See https://www.fedramp.gov/about-us/about/

- In 2016, the GAO noted in their assessment of FedRAMP that the program lacks the ability to share any best practices in order to expedite the use of currently certified CSPs
- There is a lot of uncertainty over what type of changes to the environment require re-certification.
- Outsourcing IT operations does not mean outsourcing risk – so there needs to be a component of FedRAMP that mandates the outsourcers' requirement to govern the outsourcer. If the risk is high enough, this could devolve into a near continuous monitoring proposition which most organizations lack the appetite or resources for.
- It adds another "certification" to a growing number that a Cloud Service Provider may need (e.g., PCI-DSS, SSAE-16, ISO-27001).
- The FedRAMP Joint Authorization Board JAB cannot accept risk on behalf of any agency which is why the JAB authorization is titled a "Provisional Authorization." If an agency decides to use a system with a Provisional Authorization, the agency will need to issue its own ATO letter to indicate that they accept the risk associated with using another agency's Cloud Service Provider system(s).

4.4.4.1 Supplemental and Collaborative Approach

The FedRAMP controls are based on the National Institute of Standards and Technology (NIST) Special Publication 800-53r4, which defines 17 families of Security and Privacy Controls to be used by Federal agencies. The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) provides a control framework that is aligned to the CSA guidance in 13 security domains and builds on the foundations of other industry-accepted security standards, regulations and controls frameworks such as the ISO 27001/27002, ISACA COBIT, PCI, Jericho Forum, NERC CIP as well as NIST.

In closely mapping FedRamp to security controls, Federal agencies can now better assess a cloud provider's security controls and also address what controls need to be in place to ensure the provider is compliant with FedRAMP standards[5]. The mapping will also help reduce the burden of getting the assessments and certifications for cloud vendors wanting to serve the Federal agencies. In addition, this mapping shows that 90% of the FedRAMP controls correlate to the controls defined in the CCM[25]. The documentation of this alignment will support a variety of constituents in the Federal cloud marketplace:

- Cloud Service Providers (CSPs) will be provided with guidance on how their security frameworks can be developed and documented to address the requirements of multiple assessment standards, reducing the level of effort associated with obtaining multiple security certifications;
- Assessors and auditors will be able to use the alignment to leverage documentation and artifacts to enable them to assess CSP security postures across multiple standards in an efficient manner,
- Federal agencies will be able to evaluate CSPs who have been assessed and certified against the CCM under the CSA Security Trust and Assurance Registry (STAR) program to determine the likelihood of a CSP's ability to qualify for FedRAMP certification
- The FedRAMP Program will be able to leverage the various industry standards that are integrated into the CCM framework to further the alignment of FedRAMP controls with other industry standards.

4.4.5 Cloud Security Reference Architecture

The Cybersecurity Reference Architecture (CS RA), Version 4.1, Cloud Cybersecurity Annex is intended to inform, guide, and constrain the development of solution architectures that must include cybersecurity

[25] CSA, "Cloud Security Alliance Releases Candidate Mapping of FedRamp Security Controls", https://blog.cloudsecurityalliance.org/2015/05/05/cloud-security-alliance-releases-candidate-mapping-of-fedramp-security-controls/

considerations for commercial cloud migrations and implementations; including both on-premise and off-premise CSOs. The CS RA v4.1 serves this purpose by 1) providing a common lexicon for DoD components seeking to leverage commercial cloud services, 2) identifying consistent models for policy compliant cloud service implementations, and 3) encouraging adherence to common standards to enable governance.

The DoD CS RA v4.1 presents a DoD-level, end-state vision and framework for achieving Departmental goals for secure, increasingly commercial cloud services adoption and usage to obtain IT efficiencies and improve mission effectiveness. It identifies required attributes for a single security architecture through principles, rules, technical standards, and architectural patterns.

The cybersecurity capabilities and functions relating to cloud cybersecurity identified in the CS RA v4.1 are not tied to any one organization or service provider, and instead are intended to illustrate the security environment and key policy enforcement points of which the Department must be aware when preparing to leverage CSOs. The end-state will allow for a highly flexible, highly virtualized environment which enables DoD Components to make risk decisions that are in line with DoD policy requirements. For more information on the CS RA v4.1, log into the Reference sites at https://milsuite.mil/book/groups/cyber-security-reference-architecture-working-group or https://wmaafip.csd.disa.smil.mil.

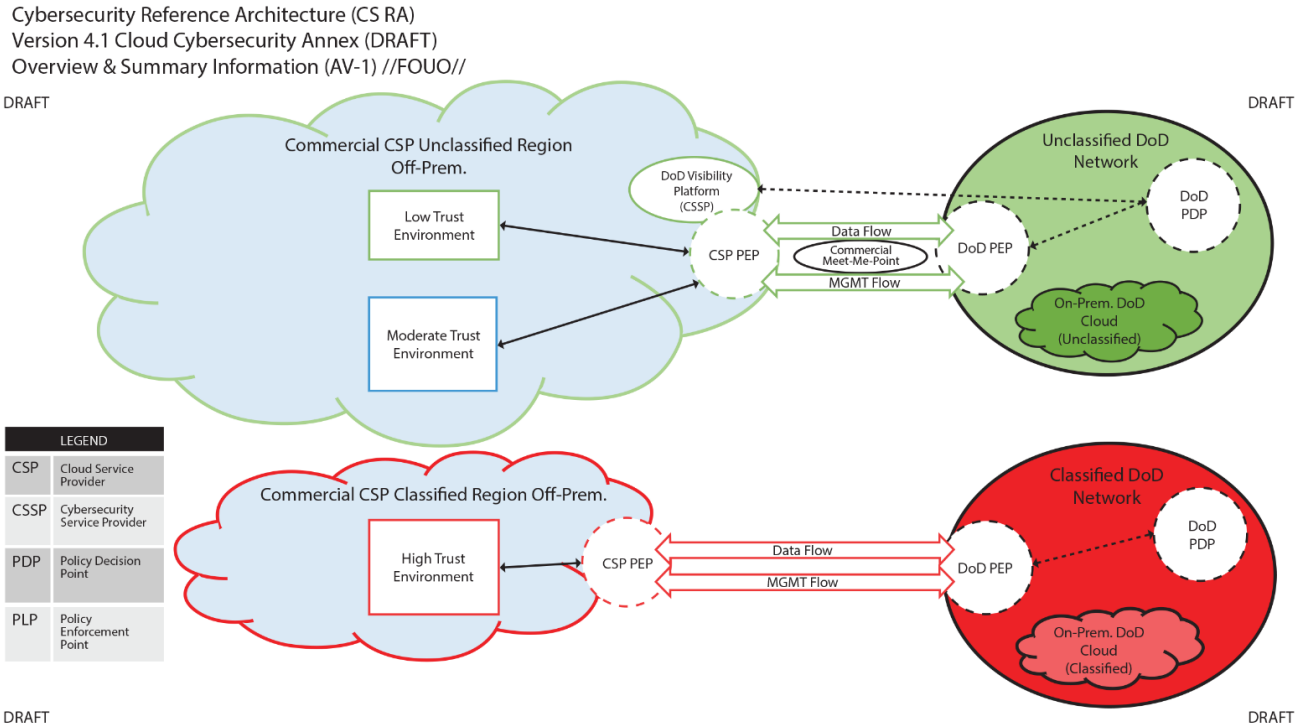


Figure 16. Cybersecurity Reference Architecture (CS RA)

4.4.6 Cybersecurity T&E

The Program should understand the cyber threats to the system that will be hosted in the cloud environment. Documented cloud security threats to commercial cloud services could also compromise cloud-hosted DoD systems. Defense contractors and governmental entities worldwide are targets regardless of which hosting environment, cloud or conventional data center. Threats heavily target the CSPs themselves, cloud computing services and data to gain access to DoD data and assets. FedRAMP, DISA PAs, CSPs, and 3PAOs provide artifacts and test results as part of FedRAMP PA process. Test planners should leverage these artifacts for planning government cybersecurity T&E. For more information about conducting cybersecurity T&E for cloud-deployed applications, see the DOD Cybersecurity T&E Guidebook v2, April 2018; Addendum: Cybersecurity T&E of DoD Systems Hosted on Commercial Cloud Service Offerings.

This page intentionally left blank

5 Service Level Agreements (SLAs)

5.1 Background

Across the public and private sector, there is no standard naming convention or structure for an SLA. The SLA is a contract between a cloud service provider and a cloud service consumer that specifies, in measurable terms, what services and guarantees the cloud provider will provide[26]. As more and more consumers migrate their internal services to cloud providers, a detailed and legal binding SLA between the parties emerge as a key characteristic of this relationship. Due to the nature of cloud offering, continuous monitoring and proper risk management are key attributes necessary to enforce SLAs. Other factors such as trust (on the cloud provider) come into play, particularly for customers that outsource its critical data to a CSPs operation. Due this complexity means of managing SLAs with the sufficient amount of IT Governance in place.

Every cloud contract (and SLA) is created to address a unique business need while addressing the security and risk management changes that the Cloud SLA must entail.

An SLA is part of a Cloud Computing agreement that:

- Defines the service and service levels being provided
- Sets performance characteristics
- Identifies metrics and how they will be measured
- Identifies guarantees and methods of redress
- Addresses federal computing and physical security requirements and
- Addresses risk management

For help in developing an SLA, refer to Appendix B: SLA Checklist.

5.2 Challenges and Best Practices

The DCOI has provided new guidance for cloud investment and shared services adoption. This new guidance complements guidance provided in the Federal Cloud Computing Strategy, which was published in February 2011. The strategy instituted the Cloud First policy, requiring agencies to evaluate cloud computing options before making new investments in physical IT infrastructure. It is intended to accelerate the adoption of cloud computing services by federal agencies and, therefore, the pace at which the government may realize the benefits of cloud adoption.[27]

In April 2016, GAO reported an assessment of how well agencies have incorporated 10 key management elements into their cloud computing service level agreements (SLAs) (See Table 2)[28]. In accordance with the Cloud First policy, FITARA, and guidance from the National Institute for Standards and Technology, the new DCOI requires agencies to use cloud infrastructure where possible when planning new applications or

[26] US Government Cloud Computing Technology Roadmap, Volume II, Release 2.0

[27] Congressional Research Service (CRS) The Current State of Federal Information Technology Acquisition Reform and Management name redacted Specialist in Internet and Telecommunications Policy, April 25, 2017

[28] U.S. Government Accountability Office, Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance,

consolidating existing applications. Agencies are encouraged to take into consideration the cost, security requirements, and application needs when evaluating cloud services.

In light of its findings, GAO recommended that:

- OMB include the 10 key practices in future guidance to agencies, and
- the Departments of Defense, Health and Human Services, Homeland Security, the Treasury, and Veterans Affairs incorporate the key practices into their SLAs.

Table 15. Key Practices for Cloud Computing Service Level Agreements[29]

Key Practices	Activities
Roles and responsibilities	1. Specify roles and responsibilities of all parties with respect to the SLA and, at a minimum, include agency and cloud providers. 2. Define key terms, such as dates and performance.
Performance measures and verification processes	1. Define clear measures for performance by the contractor. Include which party is responsible for measuring performance. Examples of such measures would include: o Level of service (e.g., service availability—duration the service is to be available to the agency). o Capacity and capability of cloud service (e.g., maximum number of users that can access the cloud at one time and ability of provider to expand services to more users). o Response time (e.g., how quickly cloud service provider systems process a transaction entered by the customer, response time for responding to service outages). 2. Specify how and when the agency has access to its own data and networks. This includes how data and networks are to be managed and maintained throughout the duration of the SLA and transitioned back to the agency in case of exit/termination of service. 3. Specify the following service management requirements: o How the cloud service provider will monitor performance and report results to the agency. o When and how the agency, via an audit, is to confirm performance of the cloud service provider. 4. Provide for disaster recovery and continuity of operations planning and testing, including how and when the cloud service provider is to report such failures and outages to the agency. In addition, how the provider will remediate such situations and mitigate the risks of such problems from recurring. 5. Describe any applicable exception criteria when the cloud provider's performance measures do not apply (e.g., during scheduled maintenance or updates).

[29] U.S. Government Accountability Office, Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance, GAO-16-325, April 2016, http://www.gao.gov/assets/680/676395.pdf

Table 15. Key Practices for Cloud Computing Service Level Agreements[29]

Key Practices	Activities
Security	1. Specify metrics the cloud provider must meet in order to show it is meeting the agency's security performance requirements for protecting data (e.g., clearly define who has access to the data and the protections in place to protect the agency's data). 2. Specify performance requirements and attributes defining how and when the cloud service provider is to notify the agency when security requirements are not being met (e.g., when there is a data breach). 3. Specify CSP support for government security verification of operational metrics and the performance metrics defined above.

5.3 The Exit Strategy

In some cases, managed IT services providers offer a subscription-based service, which means *you need to be clear on two key things*. ***First***, you'll need to know how frequently your SLA will be revised and how much warning you'll have. ***Second***, it should clearly stipulate the terms and procedures for cancelling your partnership. These critical factors may further be broken down to include things like *the secure erasure of any confidential business data in the care of your provider*. While you'll want to be looking at any IT support provider with a long-term partnership in mind, it's still crucial that you enter the contract being fully aware of the obligations of both parties *when it comes to terminating your partnership*.

5.4 Standards 19086 Series -- Service Level Agreements Standards

The International Classification for Standards (ICS) is a convention managed by the International Organization for Standardization (ISO) and used in catalogues of international, regional, and national standards and other normative documents. As part of this body of work, ICS 35 heads up Information Technology. ISC 35.210 - Cloud computing, develops the following standards on Cloud SLAs.

- ISO/IEC JTC 1/SC 38 – Cloud Computing
- 19086-1 -- Cloud computing -- Service level agreement (SLA) framework and technology -- Part 1: Overview and concepts -- Stage: Published September 2016
- 19086-2 -- Cloud computing -- Service level agreement (SLA) framework and technology -- Part 2: Metrics -- Stage: Published December 2018
- 19086-3 -- Cloud computing -- Service level agreement (SLA) framework -- Part 3: Core conformance requirements -- Stage: Published July 2017
- 19086-4 -- Cloud computing -- Service level agreement (SLA) framework and technology -- Part 4: Security and privacy – Published January 2019

5.5 SLA Fundamental Concepts and Vocabulary

- Cloud Service Agreement (CSA)
  - Documented agreement between the cloud service provider and cloud service customer that governs the covered service(s)
- Cloud Service Level Agreement (SLA)
  - Part of the cloud service agreement that includes cloud service level objectives and cloud service qualitative objectives for the covered cloud service(s)

- Cloud Service Level Objectives (SLO)
  - Commitment a *cloud service provider* makes for a specific, quantitative characteristic of a *cloud service,* where the value follows the *interval scale* or *ratio scale*
- Cloud Service Qualitative Objectives (SQO)
  - Commitment a *cloud service provider* makes for a specific, qualitative characteristic of a *cloud service* where the value follows the *nominal scale* or *ordinal scale*
- Details of cloud SLAs, SLOs and SQOs can vary for different cloud service offerings.

5.6 SLA Metrics

The definition and usage of appropriate metrics and their underlying measures and measurements are essential aspects of the cloud SLA.

- The metrics are used to set the boundaries and margins of error and limitations.
- Examples of how metrics can be used:
  - Determine if SLOs are met
  - Define a purpose for measures and measurements
  - Deliver a consistent representation of measure and measurement information
  - Link properties, measurements and metrics
  - Enable comparison of monitoring between services
  - Determine cloud service effectiveness for business objectives

5.6.1 Construction of SLAs with 19086

- Built upon selected SLA content areas.
- SLA content area is formed from a set of SLOs and SQOs.
- Each SLO & SQO has associated metrics.
- Metrics described using the NIST Cloud Metric Model.
- New cloud metrics can be constructed using this model

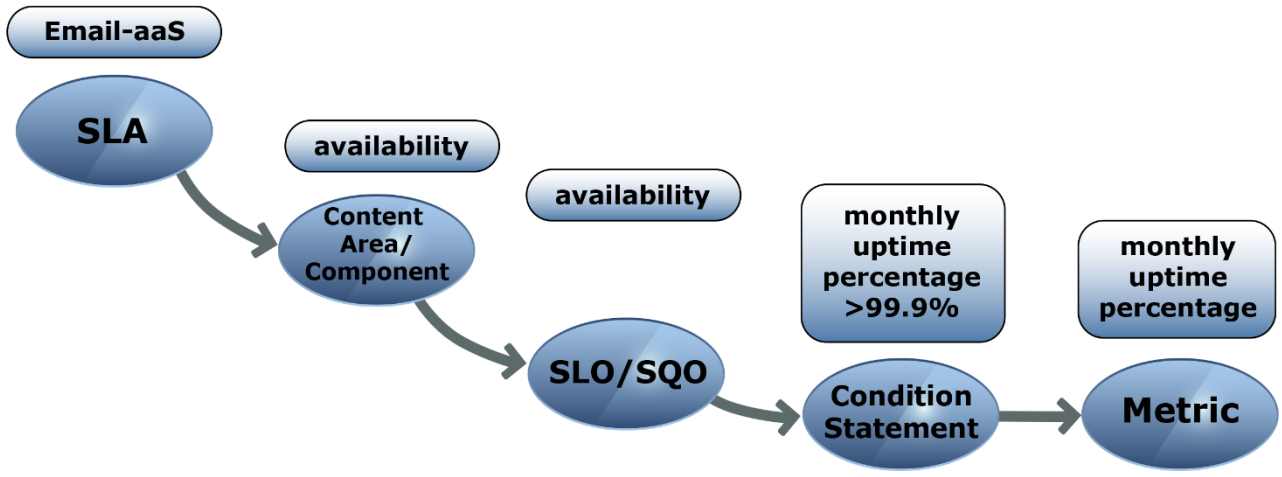


Figure 17. Constructing New Cloud Metrics

Figure 18. SLA Content Areas

5.6.2 SLA Content Areas

Table 16. SLA Content Areas and Recommended SLOs and SQOs

SLA Content Areas	Cloud SLOs	Cloud SQOs
Accessibility	Accessibility Component	• Accessibility Standards • Accessibility Policies
Attestations, Certifications, & Audits	Attestations, Certifications, & Audits	• Cloud Service Attestations • Cloud Service Certifications • Cloud Service Audits
Availability	Availability Component	• Availability
Cloud Service Support	Cloud Service Support	• Support Hours • Service Incident Support Hours • Service Incident Notification Time • Maximum First Support Response Time • Maximum Incident Resolution Time • Support Plans • Support Methods • Support Contacts • Service Incident Reporting • Service Incident Notification

Table 16. SLA Content Areas and Recommended SLOs and SQOs

SLA Content Areas	Cloud SLOs	Cloud SQOs
Data Management	Intellectual Property Rights (IPR)	• Intellectual Property Rights
	Cloud Service Customer Data	• Cloud Service Customer Data • Cloud Service Customer Data Usage •
	Cloud Service Provider Data	• Provider Data • Account Data •
	Account Data	• Derived Data • Derived Data Usage • Derived Data Access •
	Derived Data	• Data Portability Capabilities • Data Deletion Time • Data Deletion Process • Data Deletion Notification •
	Data Portability	• Data Location • Data Location Specification Capability • Data Location Policy
	Data Deletion	• Data Examination • Law Enforcement Requests
	Data Location	

Table 16. SLA Content Areas and Recommended SLOs and SQOs

SLA Content Areas	Cloud SLOs	Cloud SQOs
	Data Examination Law Enforcement Access	
Governance	Governance Component	• Regulation Adherence • Standards Adherence • Policy Adherence • Audit Schedule
Performance and verification	Cloud Service Response Time Component Cloud Service Capacity Component Elasticity Component	• Cloud Service Maximum Response Time Observation • Cloud Service Response Time Mean • Cloud Service Response Time Variance • • • Limit of Simultaneous Cloud Service Connections • Limit of Available Cloud Service Resources • Cloud Service Throughput • Cloud Service Bandwidth • Elasticity Speed • Elasticity Precision
Service Reliability and verification	Service Resilience/Fault Tolerance	• Time to Service Recovery • Mean Time to Service Recovery • Maximum Time to Service Recovery

Table 16. SLA Content Areas and Recommended SLOs and SQOs

SLA Content Areas	Cloud SLOs	Cloud SQOs
	Customer Data Backup and Restore	• Number of Service Failures • Cloud Service Resiliency/Fault Tolerance Methods • • Backup Interval • Retention Period for Backup Data • Number of Backup Generations • Backup Restoration Testing • Backup Method • Backup Verification • Backup Restoration Test Reporting • Alternative Methods for Data Recovery • Data Backup Storage Location
	Disaster Recovery	• Recovery Time Objective (RTO) • Recovery Point Objective (RPO) • Cloud Service Provider Disaster Recovery Plan
Termination of Service	Termination of Service Component	• Data Retention Period • Log Retention Period • Notification of Service Termination • Return of Assets
Change Management	Changes to the Cloud Service Features and Functionality	• Minimum Service Change Notification Period • Minimum Time Before Feature/Function Deprecation

Table 16. SLA Content Areas and Recommended SLOs and SQOs

SLA Content Areas	Cloud SLOs	Cloud SQOs
		• Service Change Notification Method
PII Protection	PII Protection Component	At the time of writing PII SLOs and SQOs are under development by JTC1 SC27 and will be included in ISO/IEC 19086-4 “Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 4: Security and privacy” when published
Information Security	Information Security Component	See Reference: DOD Cybersecurity T&E Guidebook v2, April 2018; Addendum: Cybersecurity T&E of DoD Systems Hosted on Commercial Cloud Service Offerings

The SLOs identified in the table above are not all in common use and metrics are being developed by ISO and NIST working groups. The following examples are for measurements that are in use now and could be useful in defining performance parameters for cloud contracts. As new standards for metrics are developed, this Guidebook will be updated accordingly.

5.6.2.1 Accessibility Content Area

- **Accessibility Component.** The accessibility component describes the characteristics of assistive technologies the CSP implements within a specific cloud service.
- **Service Objectives.** ISO/IEC 19086-1 lists two SQOs for accessibility:
  - **Accessibility Standards.** A statement listing accessibility related standards the CSP supports in the covered services.
  - **Accessibility Policies.** A statement listing policies and regulations for accessible ICT the CSP supports in the covered services.

5.6.2.2 Availability Content Area

- **Availability Component.** Availability is the characteristic of being accessible and usable upon demand by consumer. For a service to be useful the consumer must be able to access and use it when the need arises. This characteristic is usually provided as a percentage of time**:**

$$Availability = \frac{Ttotal - Tdowntime}{Ttotal} \; x \; 100$$

- **Service Objectives.** There is currently only one service objective for the availability characteristic included in 19086-1.
  - Monthly Uptime Percentage (Availability) (SLO)

Description: The amount or percentage of time in a given period that the cloud service is accessible and

usable. NOTE: it is also referred to as “uptime percentage” and is often given over month based billing period (i.e., monthly uptime percentage).

Important Information: This characteristic is common in current SLAs. It is an important characteristic. Although it can be complex, it can be measured without difficulty. There may be time when the service is unavailable (“down”) that does not count towards the total downtime (e.g. scheduled downtime). It is important to understand what counts as unavailable and how the unavailable periods are combined.

Compute resources are often described using the time-based concept of availability while storage resources are often described using the transaction-based concept of availability.

Example hours unavailable for common monthly uptime percentages (based on a thirty day month):

- 99.99% would be 4 minutes unavailable in a month
- 99.95% would be 6.5 minutes unavailable in a month
- 99.9% would be 43 minutes unavailable in a month
- 99% would be 432 minutes unavailable in a month

5.6.2.3 Cloud Service Performance Content Area

- **Cloud Service Response Time Component Description.** Cloud Service Response Time is the time interval between a stimulus to the cloud service and the service’s response to the stimulus. Response time is important for cloud computing services because consumers need to get a response to each request in a timely manner – if it takes too long to get the result it may no longer be useful. From the consumer’s perspective this would be best measured at the edge of the consumer’s IT system. Measuring response time from this point includes the network transit time for both the request and the response. The following equation assumes equal transit time for both:

  $$Tcsrt = 2Ttt + Trt$$

  (where Tcsrt is the instantaneous cloud service response time, Ttt is the total network transit time and Trt is the server side response time). Because no rules on how to measure each of these times are provided in the above example it is not clear whether this includes the time it takes for all the bits of the message to be transmitted. If the request and response are small (few bits) the additional time for the full message to be transmitted is small, but if the messages are large (e.g. such as image or video files) the time to transfer all the bits may be significant.

From the above equation, it can be seen how important for the consumer to consider that while a CSP may only commit to a level of response time within their systems, the effects of the connecting network and the consumers systems/networks must be understood for the consumer to understand the effective response time in a given application. While a consumer may be concerned about the total response time as measured on their system side (and shown in the above equation), the CSP is not likely to provide this information. The CSP has not control (or responsibility) over the connecting networks. To have a complete understanding of response time the consumer should get transit time data from the network provided, response time data from the CSP, and make response time measurements at the edge of the consumer’s own systems. When defining or measuring response time it is important to know where/when the stimulus is being observed and where/when the response is being observed.

- Service Objectives
    - **Cloud Service Maximum Response Time Observation (SLO).** The maximum time between a defined stimulus or input to the cloud service and a defined point in the response.

The commitment the providers should give to provide a service where the measured service characteristic is lower than commitment value.

- **Important Information:** This characteristic is not common in current SLAs but it may be used as part of the availability SLO to determine whether the service is available (i.e. If the response takes too long, the service is considered unavailable). It is an important characteristic and can be measured without difficulty. It is important to recognize that a request to the CSP might never arrive due to networking issue. So, from the customer's point of view, any service maximum response time might be exceeded, but in fact the CSP never received the request. This value should take into consideration both the CSP response time as well as the network response time.

Include cloud service maximum response time in the SLA. The commitment value should be based on the customer requirements and consider the effects of network transit time. Use Metric T1 or T2. (see metric catalog TBA).

- T1: Measurement starts when CSP receives request in full and measurement stops when the CSP starts to send the response.
- T2: Measurement starts when CSP receives request in full and measurement stops when the CSP finishing sending the response. Any commitment made using Y2 will be dependent on the size of the response.

5.6.2.4 Capacity Component

The capacity component covers characteristics of cloud services including; storage space, processing power, simultaneous connections, service bandwidth and throughput. ISO/IEC 19086-2 contains the following SLOs:

- Maximum number of simultaneous connections supported
- Maximum capacity of available resources
- Cloud Service Throughput
- Cloud Service Bandwidth

5.6.2.5 Protection of PII Content Area

- **Protection of PII Component:** The capability of the cloud computing service to protect personally identifiable information (PII). PII is defined in NIST SP 800-122 as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."
- **Important Information:** Protection of PII and PII management are important concepts and some language related to PII is likely included in a cloud contract in a clause or SOO/SOW/PWS.

PII (SO)

At the time of writing PII SLOs and SQOs are under development by JTC1 SC27 and will be included in ISO/IEC 19086-4 "Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 4: Security and privacy" when published.

This page intentionally left blank

6 Existing DoD Contracts and POCs

Table 17 provides current information on existing and upcoming DoD contracts that can be used to acquire cloud services, depending on your organization.

Table 17. DoD Cloud Contracting Vehicles

DoD Agency/Service	Contract Vehicle	Point(s) of Contact
Defense Information Systems Agency (DISA):		
Office: Defense Information Systems Agency (DISA) Ft Meade, MD 20755 United States DITCO-NCR	Defense Enterprise Office Solutions (DEOS) (Microsoft Office 365 SaaS) Status: Awarded to GDIT August 2019 – ***Under Protest*** Corrective Action Being Taken MILCloud 2.0 (Awarded to GDIT)	DEOS Program Management Office (PMO) Email: disa.meade.sd.mbx.defense-enterprise-office-automation-deos@mail.mil (DEOS Contract Award and Administration moved to GSA so that non DoD programs can access the contract.) https://www.disa.mil/Computing/Cloud-Services
Defense Logistics Agency (DLA):		

Table 17. DoD Cloud Contracting Vehicles

DoD Agency/Service	Contract Vehicle	Point(s) of Contact
Office: DLA Acquisition Location: DLA Contracting Services Office in Philadelphia, PA	DLA Cloud Access Point (CAP) Support Project Solicitation Number: SP4701-16-R-0063	Primary: James T. Smith, Contracting Officer James.T2.Smith@dla.mil Phone: 215.737.2713 Secondary: Brian Dudek, Contracting Officer brian.dudek@dla.mil Phone: 215.737.5872
Office: DLA Acquisition Location: DLA Contracting Services Office in Philadelphia, PA	DLA Cloud Based Electronic Document Scanning Solicitation Number: SP4701-18-R-0100	James T. Smith, Contracting Officer James.T2.Smith@dla.mil Phone: 215.737.2713
Department of Defense (DoD)		
Other Defense Agencies Office: Washington Headquarters Services Location: WHS, Acquisition Directorate	Joint Enterprise Defense Infrastructure (JEDI) Cloud RFP Solicitation Number: HQ003418R0077_JEDI_CLOUD_RFP Contract Awarded to Microsoft October 26, 2019 Protests possible – ordering date TBD.	Primary Point of Contact.: Rashida D. Webb, Contract Specialist rashida.d.webb.civ@mail.mil Phone: 7035453351
Department of the Air Force:		
Air Force's Cloud One	Cloud One Kickstart homepage	https://intelshare.intelink.gov/sites/afcc

Table 17. DoD Cloud Contracting Vehicles

DoD Agency/Service	Contract Vehicle	Point(s) of Contact
		e/Pages/Home.aspx ANDREW DOYE, GS-14, DAF SAF/CNSE, Compute & Store Portfolio Pentagon, Suite 4D755 DSN: 222-6172 Comm: 703-692-6172
Office: PEO C3I&N Location: Hanscom AFB, MA	Cloud Hosted Enterprise Services (CHES) (MS Exchange, Skype for Business, SharePoint Online, One Drive)	Alan Tocito, Contracting Officer Alan.tacito@us.af.mil Phone: 781.225.4093
Office: PEO C3I&N Location: Hanscom AFB, MA	Enterprise IT as a Service (EITaaS) - OTA	Alan Tocito, Contracting Officer Alan.tacito@us.af.mil Phone: 781.225.4093
The AFLCMC LevelUP Branch at JBSA-Lackland, TX, has been tasked to acquire Cloud Services. The Contractor shall perform all activities required to meet the requirements identified in the Statement of Objectives. The period of performance will consist of a five (5) year ordering period from date of BPA issuance. The performance period for all Calls placed under this BPA shall not exceed five (5) years from the completion of the ordering period.	Cloud Services Blanket Purchase Agreement Solicitation Number: FA8307-19-R-0135 Agency: Department of the Air Force Office: Air Force Materiel Command Location: AFLCMC – Hanscom Status: RFQ released Sept 2019 for 15 BPAs – Responses were due Oct 2019. ($95M)	Contracting Office Address: 9 Eglin Street Hanscom AFB, Massachusetts 01731 United States Primary Point of Contact.: Christina Fernandez, Contract Specialist christina.fernandez@us.af.mil Phone: 2109251088

Table 17. DoD Cloud Contracting Vehicles

DoD Agency/Service	Contract Vehicle	Point(s) of Contact
Department of the Army:		
Office: Army Corps of Engineers Location: USACE HNC, Huntsville, AL	Cloud Services Support - DC Solicitation Number: W912DY18R6000	Primary: Arlene Brown arlene.brown@usace.army.mil Phone: 256.895.1234 Secondary: Christopher Barnett christopher.m.barnett@usace.army.mil Phone: 256.895.1454
Office: Army Program Executive Office- Enterprise Information Systems (PRO EIS)	Basic Ordering Agreement (BOA) Army Cloud Computing Enterprise Transformation (ACCENT) contract vehicle	Primary: Joanne Curry, PEO EIS 703-704-1497
Department of the Navy:		
Navy Cloud Broker Office Program Manager: Travis Methvin PMW 270 Navy Commercial Cloud Services PEO EIS	Onboarding Team: william.karstens@navy.mil	https://cloud.navy.mil : **Military Sealift Command** Gregory Florence Gregory.florence@navy.mil Samuel Kovacic Samuel.kovacic@navy.mil **Naval Air Systems Command**

Table 17. DoD Cloud Contracting Vehicles

DoD Agency/Service	Contract Vehicle	Point(s) of Contact
		Support Contact: Damon Harding Damon.harding@navy.mil **Naval Information Warfare Systems Command** **Support Contact:** Darlene Shaw Darlene.shaw@navy.mil Richard Jack (NIWC Pac) Richard.jack@navy.mil Teri-Lee Holland (NIWCLant) Teri-lee.holland@navy.mil
Office: U.S. Marine Corps Location: MCCS HQMC, Personal and Family Readiness Division (MR)	MCCS Cloud Computing Initiative Solicitation Number: H0117-I-0006	Aurea I Torres Jones, Contract Specialist aureairis.torresjones@usmc-mccs.org Phone: 703.784.3804
Office: U.S. Navy PEO EIS Naval Enterprise Networks (PMW-205)	This BPA was issued against CSRA's General Services Administration (GSA) Schedule 70 contract (GS-35F-393CA)	Decentralized Ordering following the Navy Cloud Brokerage Policy (Policy is listed in Appendix F: References)
Other Defense Agencies:		

Table 17. DoD Cloud Contracting Vehicles

DoD Agency/Service	Contract Vehicle	Point(s) of Contact
General Services Administration DEOS - Defense Enterprise Office Solutions (DEOS) GSA IT Schedule 70	-GSA leads contracting activities -DEOS PMO with DoD Services leads technical evaluations leading to BPA award -DEOS PMO leads stand up, technical integration, testing, and configuration management -Services will work directly with GSA to issue Task Orders for migration of their services Cloud Special Item Number (SIN) 132-40 https://www.gsa.gov/technology/technology-purchasing-programs/it-schedule-70/sins-and-solutions-we-offer/cloud-special-item-number-sin-13240	DEOS Program Management Office (PMO) Email: disa.meade.sd.mbx.defense-enterprise-office-automation-deos@mail.mil Call: 855-482-4348 Hours for live chat and calls: Sun 8 p.m. - Fri 8:30 p.m. CST Email: ITCSC@gsa.gov
Office: USCYBERCOM Location: USCYBERCOM Contracting	Big Data Platform (BDP) Engineering and Development Services Solicitation Number: HB000118R0001	Primary: Kelly A. Beck, Head of Contracting Activity kabeck@cybercom.mil Phone: 301.688.2103 Secondary:

Table 17. DoD Cloud Contracting Vehicles

DoD Agency/Service	Contract Vehicle	Point(s) of Contact
		Nichole C. Cabral, Contract Specialist nccabra@cybercom.mil Phone: 443.634.0751
Office: U.S. Transportation Command Location: USTRANSCOM Command Acquisition	Cloud Computing Services Solicitation Number: HTC711-17-ZD03	Primary.: Kendra N. Taylor, Contract Specialist kendra.n.taylor2.civ@mail.mil Phone: 6182206729 Secondary: Pamela S Hall, Director, Small Business Programs pamela.s.hall32.civ@mail.mil Phone: 618.220.7066
Office: U.S. Transportation Command Location: USTRANSCOM Command Acquisition	Cloud Services (SC2S) Solicitation Number: TRANSCOM18D005	Pamela S Hall, Contracting Officer pamela.s.hall32.civ@mail.mil Phone: 618-220-7066

This page intentionally left blank

Appendix A: Representative Example Contract Clauses

This appendix provides specific contract clauses that constitute a representative (but not comprehensive) sample applicable to cloud hosted IT systems contracted under the Department of Defense (DoD). The description column provides a categorization of the clause and the columns on the right provide guidance on the source and/or section applicability. Specific column abbreviations are defined here:

- **Add'l Info Req'd**: Indicates the clause requires additional information.
- **CDRL**: Applicable to the Contract Data Requirements List.
- **DFAR**: Clause originates in the Defense Federal Acquisition Regulation Supplement (DFARS).
- **IR**: Part of an Interim Rule that should be removed when updated in the DFARS.
- **PWS**: Are applicable to performance work statements.
- **SLA**: Applicable to service level agreements.
- **SRG**: Clause originates within the DoD Cloud Computing Security Requirements Guide.

Additionally, within the clauses, the following terms are further defined:

- "Configuration control" means having the authority to approve or disapprove any and all changes to the hardware and software used in the data repository systems.
- "Operational control" means having the authority over the components of the data repository systems to include the hardware, software, processes, and personnel used to process or store government data.

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
Asset Availability	(1) The Contractor must inform the Government of any interruption in the availability of the cloud service as required by the service level agreement.			X		X	
Asset Availability	(2) Whenever there is an interruption in service, the Contractor must inform the Government of the estimated time that the system or data will be unavailable. The estimated timeframe for recovery of the service must be related to the FIPS 199 system categorization for the availability of the system and if specified, agreed upon service level agreements (SLA) and system availability requirements. The Contractor			X		X	

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
	must provide regular updates to the Government on the status of returning the service to an operating state according to the agreed upon SLAs and system availability requirements.						
Asset Availability	(3) The Contractor shall be responsible for maintaining and ensuring continued compatibility and interoperability with the Government's systems, infrastructure, and processes for the term of the contract. In the event of an unavoidable compatibility and interoperability issue, the Contractor shall be responsible for providing timely notification to the Government and shall be responsible for working with the Government to identify appropriate remedies and if applicable, work with the Government to facilitate a smooth and seamless transition to an alternative solution and/or provider.			X		X	
Banner	The Standard Mandatory DoD Notice and Consent Banner will be displayed at log on to all DoD information systems. Choose either banner a or b based on the character limitations imposed by the			X			

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
	system. The formatting of these documents, to include the exact spacing between paragraphs, must be maintained. The banner shall be implemented as a click-through banner at logon (to the extent permitted by the operating system), meaning it prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating “OK.”						
Banner	a. [Use this banner for desktops, laptops, and other devices accommodating banners of 1300 characters.]			X			
Banner	You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.			X			
Banner	By using this IS (which includes any device attached to this IS), you consent to the following conditions:			X			
Banner	- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and			X			

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
	counterintelligence (CI) investigations						
Banner	- At any time, the USG may inspect and seize data stored on this IS			X			
Banner	- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.			X			
Banner	- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.			X			
Banner	- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.			X			
Banner	OK			X			

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
Banner	b. [For Blackberries and other PDAs/PEDs with severe character limitations:]			X			
Banner	I've read & consent to terms in IS user agreement.			X			
Continuous Monitoring	The Contractor will provide all reports required to be completed; including self-assessments required by the FedRAMP Continuous Monitoring Strategy Guide to the Agency's designated security point of contact. In addition, the Government may request additional reports based on data required to be collected by FedRAMP's continuous monitoring requirements. If requested, the Contractor will provide the report to the Government within 10 business days.			X			x
Cybersecurity Compliance	The Contractor will ensure that its environment is compliant with the control standards of FISMA (Federal Information Security Management Act) 44 U.S.C. § 3541, et seq.) , NIST standards in FIPS 140-2, FIPS 180, FIPS 198-1, FIPS 199, FIPS 200, FIPS 201 and NIST Special Publications 800-53, 800-59, and 800-60 and with agency management directive DODI 8500.1. In addition, the Contractor must provide the			X			

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
	Government with any documentation it requires for its reporting requirements within 10 days of a request.						
Cybersecurity Compliance	The Contractor will ensure that the cloud environment fully complies or exceeds the security requirements for level ___in the DoD Cloud Security Model SRG. The Contractor will make the environment accessible for a DoD security team to evaluate the environment prior to the placement of any DoD data in the environment and allow for periodical security reviews of the environment during the performance of this contract.		X				
Data Breach and Incident Reporting/PIA	DFAR 252.239.700x		X				
Data Breach and Incident Reporting/PIA	The Contractor shall adopt and maintain administrative, technical, and physical safeguards and controls to protect and remedy data breaches, if any, of Government data. The Contractor will submit reports of cyber incidents through approved reporting mechanisms, as specified in CJCSM 6510.01B, Enclosure C, Section 4. The Contractor's existing notification		X				x

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
	mechanisms that are already in place to communicate between the Contractor and its customers for some or all classes of CND information may be used, as long as those mechanisms demonstrate a level of assurance, equivalent to the listed encrypted mechanisms, for the confidentiality and integrity of the information.						
Data Breach and Incident Reporting/PIA	The Contractor will apply the template format specified in CJCSM 6510.01B, Appendix B to Enclosure C, Section 1 – General Cyber Incident Report Format when reporting initial incidents by secure fax, telephonically, or by other electronic means. Initial reports may be incomplete. Reporting should balance the necessity of timely reporting (reports with critical information) versus complete reports (those with all blocks completed). Timely reporting is vital, and complete information should follow as details emerge.		X				
Data Breach and Incident Reporting/PIA	In addition to the above, if the incident concerns a breach of PII or a potential breach of PII, the Contractor will report to the contracting officer's designee within 60 minutes of the		X				

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
	discovery of any data breach. The Contractor shall provide the Government with all information and cooperation necessary to enable compliance by the Contractor and/or the Government with data breach reporting and mitigation actions required by applicable law, regulation, policy, and this contract.						
Facility Inspections	The Contractor agrees to have an independent third party or other industry recognized firm, which has been approved by the Government conduct a security audit based on the Government's criteria at least once a year. The audit results and Contractor's plan for addressing or resolving of the audit results shall be shared with the Government within 20 days of the Contractor's receipt of the audit results. In addition, the Government reserves the right to inspect the facility to conduct its own audit or investigation.		X	X			
Indemnification	(1) The Contractor shall indemnify the Government and its officers, agents, and employees acting for the Government against any liability arising out of the performance of this contract, including costs			X			

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
	and expenses, incurred as the result of the Contractor's unauthorized introduction of copyrighted material, information subject to a right of privacy, and any libelous or other unlawful matter into Government data. The Contractor agrees to waive any and all defenses that may be asserted for its benefit, including (without limitation) the Government Contractors Defense.						
Indemnification	(2) The Contractor shall indemnify the Government and its officers, agents, and employees acting for the Government against any liability arising out of the performance of this contract, including costs and expenses, incurred as the result of (i) the Contractor's unauthorized disclosure of trade secrets, copyrights, contractor bid or proposal information, source selection information, classified information, material marked "For Official Use Only", information subject to a right of privacy or publicity, personally identifiable information as defined in OMB Memorandum M-07-19 (July 12, 2006), or any record as defined in 5 U.S.C. § 552a; or (ii) the Contractor's			X			

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
	unauthorized introduction of any libelous or other unlawful matter into Government data. The contractor agrees to waive any and all defenses that may be asserted for its benefit, including without limitation the Government Contractors Defense.						
Indemnification	(3) In the event of any claim or suit against the Government on account of any alleged unauthorized disclosure or introduction of data or information arising out of the performance of this contract or services performed under this contract, the Contractor shall furnish to the Government, when requested by the Contracting Officer, all evidence and information in the Contractor's possession pertaining to such claim or suit. Such evidence and information shall be furnished at the expense of the Contractor; provided, however, that an equitable adjustment shall be made under this clause, and the contract modified in writing accordingly, if the claim or suit is withdrawn, settled, or adjudicated in favor of the Government, and the basis for the claim or suit, regardless of outcome, was not due to any			X			

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
	act or omission of the Contractor.						
Indemnification	(4) The provisions of this paragraph do not apply unless the Government provides notice to the Contractor as soon as practicable of any claim or suit, affords the Contractor an opportunity under applicable laws, rules, or regulations to participate in the defense of the claim or suit, and obtains the Contractor's consent to the settlement of any claim or suit other than as required by final decree of a court of competent jurisdiction; and these provisions do not apply to any libelous or other unlawful matter contained in such data furnished to the Contractor by the Government and incorporated in data to which this clause applies. Further, this indemnity shall not apply to—			X			
Indemnification	a. A disclosure or inclusion of data or information upon specific written instructions of the Contracting Officer directing the disclosure or inclusion of such information or data;			X			
Indemnification	b. A third-party claim that is unreasonably settled without the consent of the Contractor, unless required by final decree of a court of competent			X			

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
	jurisdiction.						
Insurance	(1) The Contractor shall provide and maintain insurance, to include cybersecurity insurance, throughout the performance of this contract, as specified in the Schedule or elsewhere in the contract.			X			
Insurance	(2) Before commencing performance under this contract, the Contractor shall provide proof of insurance to the Contracting Officer. The Contractor shall resubmit the proof of insurance within 30 days of notification of any material change that occurs during the performance of the contract.			X			
Insurance	(3) The Contractor shall insert the substance of this clause, including this paragraph (c), in subcontracts under this contract that require work with or in support of storage and retrieval of electronic/digital government data and shall require subcontractors to provide and maintain the insurance required in the Schedule or elsewhere in the contract. The Contractor shall maintain a copy of all subcontractors' proofs of required insurance and shall make copies available to the			X			

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
	Contracting Officer upon request.						
Law Enforcement	(1) The Contractor shall record all physical access to the cloud storage facilities and all logical access to the government data as specified in the Schedule. This may include the entrant's name, role, purpose, account identification, entry and exit time. Such records shall be provided to the Contracting Officer or designee in accordance with the Schedule or upon request to comply with federal authorities.			X			
Law Enforcement	(2) As specified by the Contracting Officer, the Contractor shall provide immediate access to all Government data and Government-related data impacting Government data for review, scan, or conduct of a forensic evaluation and physical access to any contractor facility with Government data. If the Government data is co-located with the non-Government data, the Contractor shall isolate the Government data into an environment where it may be reviewed, scanned, or forensically evaluated in a secure space with access limited to authorized			X			

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
	Government personnel identified by the Contracting Officer, and without the Contractor's involvement.						
Location of Data	(1) The Contractor shall maintain all data within the United States, which means the 50 States, the District of Columbia, and outlying areas.		X				
Location of Data	(2) The Contractor shall provide the Government with a list of the physical locations which may contain government data within 20 days with updates on a quarterly basis.		X				X
Maintenance	The Contractor shall be responsible for all patching and vulnerability management (PVM) of software and other systems' components supporting services provided under this agreement so as to prevent proactively the exploitation of IT vulnerabilities that may exist within the Contractor's operating environment. Such patching and vulnerability management shall meet the requirements and recommendations of NIST SP 800-40, as amended, with special emphasis on assuring that the vendor's PVM systems			X		X	

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
	and programs apply standardized configurations with automated continuous monitoring of the same to assess and mitigate risks associated with known and unknown IT vulnerabilities in the Contractor's operating environment. Furthermore, the Contractor shall apply standardized and automated acceptable versioning control systems that use a centralized model to capture, store, and authorize all software development control functions on a shared device that is accessible to all developers authorized to revise software supporting the services provided under this agreement. Such versioning control systems shall be configured and maintained so as to assure all software products deployed in the Contractor's operating environment and serving the Government are compatible with existing systems and architecture of the Government.						
Misuse of Government Data and Metadata	(1) The Contractor shall not access, use, or disclose Government data unless specifically authorized by the terms of this contract or a task order issued hereunder. If authorized by the terms of this	X	X				

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
	contract or a task order issued hereunder, any access to, or use or disclosure of, Government data shall only be for purposes specified in this contract or task order. Contractor shall ensure that each of its employees and representatives, and any others (e.g., subcontractor employees) performing duties hereunder, shall, prior to obtaining access to any Government data, sign a contract or task order specific nondisclosure agreement.						
Misuse of Government Data and Metadata	(2) The Contractor shall use Government-related data only to manage the operational environment that supports the government data and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer.	X	X				
Misuse of Government Data and Metadata	(3) A breach of the obligations or restrictions set forth in (b)(1) and (b)(2) may subject the Contractor to criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and any other appropriate remedies by any party adversely affected by the breach.	X					
Non-Disclosure	See number 6, Organizational Conflict of Interest. Ensure that			X			

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
Agreements	all contractors sign an NDA.						
Notification	The Contractor shall notify the Government within 60 minutes of any warrants, seizures, or subpoenas it receives, including those from another Federal Agency that could result in the loss or unauthorized disclosure of any Government data. The Contractor shall cooperate with the Government to take all measures to protect Government data from any loss or unauthorized disclosure that might reasonably result from the execution of any such warrant, seizure, subpoena, or similar legal process.	X					
Personnel Access	The Contactor will require all employees who will have access to government data, the architecture that supports government data, or any physical or logical devices/code to pass the appropriate background investigation required by the Government in compliance with HSPD -12. At a minimum, all Contractor employees with access to the government data, the architecture that supports government data, or any		X[30]		X		

[30] Referenced in existing clause.

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
	physical or logical devices/code will pass a NACI investigation and be a US person as defined in Executive Order 12333.						
Physical Access	(1) The Contractor shall record all physical access to the cloud storage facilities and all logical access to the government data as specified in the Schedule. This may include the entrant's name, role, purpose, account identification, entry and exit time. Such records shall be provided to the Contracting Officer or designee in accordance with the Schedule or upon request to comply with federal authorities.		X				x
Physical Access	(2) As specified by the Contracting Officer, the Contractor shall provide immediate access to all Government data and Government-related data impacting Government data for review, scan, or conduct of a forensic evaluation and physical access to any contractor facility with Government data. If the Government data is co-located with the non-Government data, the Contractor shall isolate the Government data into an environment where it may be reviewed, scanned, or forensically evaluated in a		X				

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
	secure space with access limited to authorized Government personnel identified by the Contracting Officer, and without the Contractor's involvement.						
Records	(1) The Contractor shall provide the Contracting Officer all Government data and Government-related data in the format specified in the Schedule or as directed by the Contracting Officer.	X					x
Records	(2) The Contractor shall dispose of Government data and Government-related data in accordance with the Schedule and provide the confirmation of disposition to the Contracting Officer in accordance with contract closeout procedures.	X					
Records	(3) The Contracting Officer may at any time issue a hold notification in writing to the Contractor. At such time, the Contractor may not dispose of any Government data or Government-related data described in the hold notification until such time as the Contractor is notified in writing by the Contracting Officer and shall preserve all such data in accordance with agency instructions.			X			

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
Records	(4) The Contractor shall provide the Contracting Officer within 10 business days of receipt of any requests from a third party for Government-related data.			X			
Records	(5) When the Government is using a Contractor's software, the Contractor shall provide the agency with access and the ability to search, retrieve, and produce Government data in a standard commercial format.			X			
Spillage	(1) Upon written notification by the Government of a spillage, the Contractor shall coordinate immediately with the responsible Government official to correct the spillage in compliance with agency-specific instructions.	X					
Spillage	(2) If the Contractor incurs additional cost to correct the spillage, or the effort to correct the spillage causes a delay in the performance of any part of the work under this contract, and such costs or delays were not caused by any act or omission of the Contractor, an equitable adjustment shall be made under this clause and the contract modified in writing accordingly.	X					

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
Spillage	(3) No request by the Contractor for an equitable adjustment to the contract under this clause shall be allowed, unless the Contractor has given a written notice thereof within 30 days after the notification prescribed in paragraph (a) of this clause.	X					
Spillage	(4) No request by the Contractor for an equitable adjustment to the contract due to a spillage shall be allowed if made after final payment under this contract.	X					
Spillage	(5) Any spill of data by the Contractor into the environment hosting Government Data, will be immediately reported to the Government POC (insert POC) and the Contractor will follow the Government's instructions to clean up the spill at the Contractor's expense.	X					
Supply Chain	(1) Supply Chain Risk Management (SCRM) Plan. The offeror shall submit a SCRM plan as part of its technical proposal. The SCRM plan shall describe the offeror's approach to SCRM and demonstrate how the offeror's approach will reduce and mitigate supply chain risks. The SCRM plan shall address:			X			

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
Supply Chain	a. System Security Engineering. The SCRM plan shall describe the offeror's use of system security engineering processes in specifying and designing a system that is protected against external threats and against hardware and software vulnerabilities.			X			
Supply Chain	b. Criticality Analysis. The SCRM plan shall include the criticality analysis (CA) process used by the offeror to determine Mission Critical Functions and the protection techniques (countermeasures and sub-countermeasures) used to achieve system protection and mission effectiveness. The CA shall describe the offeror's supply chain for all critical hardware and software components (and material included in products), key suppliers, and include proof of company ownership and location (on-shore or off-shore) for key suppliers and component manufacturers. The CA shall identify critical functions and components (hardware, software, and firmware) in accordance with both DoDI 5200.44 "Protection of Mission critical Functions to Achieve Trusted Systems and Networks (TSN)". Criticality			X			

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
	levels that support the CA are defined in the document "Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, "program Protection Plan Outline and Guidance," July 18, 2011.						
Supply Chain	c. SCRM Security Controls. The SCRM plan shall describe the offeror's strategy for implementing of SCRM security requirements throughout the life of the contract. The SCRM plan shall address the security controls (at a minimum SA-12) described in National Institute of Standards & Technology (NIST) Special Publication 800-53 Revision 4 (current version), Recommended Security Controls for Federal Information Systems and Organizations (http://csrc.nist.gov/publications/PubsSPs.html), and should be tailored in scope to the effort and the specific unclassified DoD information.			X			
Supply Chain	d. Delivery Mechanisms. The SCRM plan shall describe the offeror's physical and logical delivery mechanisms to protect against unauthorized access, exposure of system components, information misuse, unauthorized			X			

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
	modification, or redirection;						
Supply Chain	e. Operational and Disposal Processes. The SCRM plan shall describe the offeror's operational processes (during maintenance, upgrade, patching, element replacement, or other sustainment activities) and disposal processes that limit opportunities to knowledge exposure, data release, or system compromise.			X			
Supply Chain	f. SCRM Training/Awareness Program.			X			
Supply Chain	(2) Contractor-Manufacturer Relationship. The SCRM plan shall identify the relationship between the offeror and the manufacturer as one of the following: (1) OEM; (2) authorized reseller; (3) authorized partner/distributor; or (4) unknown/unidentified source.			X			
Supply Chain	(3) Malicious Code Warranty. The SCRM plan shall include the offeror's expressed warranty that the software shall be free from all computer viruses, worms, time-outs, time bombs, back doors, disabling devices and other harmful or malicious code intended to or which may damage, disrupt,			X			

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
	inconvenience or permit access to the software user's or another's software, hardware, networks, data or information.						
Supply Chain	(4) Subcontracts. The Offeror shall incorporate the substance of this clause in subcontracts at all tiers where a subcontractor provides personnel, components or processes identified as either a critical component or its supporting infrastructure. All subcontractors providing critical components or services shall be identified and required to provide all necessary information to complete the SCRM Plan in association with the Offeror.			X			
Supply Chain	(5) SCRM Plan Submission & Review. The SCRM plan and supporting documents shall be submitted to the contracting officer as part of the offeror's technical proposal. All SCRM plans and appropriately marked related information will be treated as proprietary information by the Government and handled as Controlled Unclassified Information pursuant to Executive Order 13556 and shall be used solely for the purposes of managing risk to Government Functions.			X			

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
	The government shall review the offeror's SCRM plan to determine whether the SCRM plan demonstrates an acceptable methodology for managing supply chain threats/risks. The SCRM plan review shall consider the offeror's SCRM approach for: (1) System Security Engineering; (2) Criticality Analysis; (3) SCRM Security Controls; (4) Delivery Mechanisms; (5) Operational and Disposal Processes; and (5) SCRM Training/Program Awareness. The SCRM plan must be deemed acceptable by the contracting officer in order for the offeror to be eligible for award. The offeror's failure to submit an acceptable SCRM plan may result in the offeror being eliminated from further consideration for contract award.						
Supply Chain	(6) Material Term of the Contract. Failure by the offeror to submit an acceptable SCRM Plan with its proposal may result in the offeror's exclusion from award. Failure by the Contractor to execute, maintain and distribute a current SCRM Plan for review by the Government in accordance with the terms of the contract shall			X			

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
	constitute a material breach of the contract and may result in termination for default or cause.						
Terms of Service	Use FAR Clause: 52.212-4(u): The following shall supersede any language in the Contractor's commercial terms of service:		X				
Terms of Service	(1) Confidentiality. The Government, to the extent permitted by law and regulation, will safeguard and treat information obtained pursuant to the Contractor's disclosure as confidential where the information has been marked "confidential" or "proprietary" by the company. To the extent permitted by law and regulation, such information will not be released by the Government to the public pursuant to a Freedom of Information Act request, 5 U.S.C. § 552, without prior notification to the Contractor. The Government may transfer documents and information provided by the Contractor to any department or agency within the Executive Branch if the information relates to matters within the organization's jurisdiction.		X				

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
Terms of Service	(2) Disputes and governing law. Any and all other terms or conditions notwithstanding, disputes arising under or relating to this contract or agreement are subject exclusively to Federal law, particularly the Contract Disputes Act of 1978, as amended (41 U.S.C. §§ 7101-7109) (the Act) and the provisions of 48 CFR subpart 33.2. Except as provided in the Act, all disputes arising under or relating to this contract shall be resolved under the clause set forth at 48 CFR 52.233-1.			X			
Terms of Service	(3) Other legal matters. Any and all other terms or conditions notwithstanding, legal actions in which the Government is a party that do not arise under or relate to this contract or agreement shall be prosecuted under applicable Federal law in the appropriate Federal venue.			X			
Terms of Service	(4) Endorsement. The Contractor may not use the name, seal, logo or other readily identifiable indicia of any Government agency or organization in such a way that may be construed as advertising or endorsement by the Government of the			X			

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
	Contractor. The Contractor may include within a list or display of the Contractor's customers for the purposes of advertising or publicity the names, seals, logos or other indicia of Government agencies and organizations that have entered into contracts with the Contractor. However, it must not be stated or implied that the Government in any way recommends or endorses the products or services of the Contractor						
Terms of Service	(5) Indemnification and renewal. Any other terms or conditions notwithstanding, this contract or agreement shall not and does not require the Government to (i) indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability, which would violate the Anti-Deficiency Act (31 U.S.C. § 1341) (ADA), or (ii) automatically renew this contract or agreement at any time in the future, which would violate the ADA. Any such provisions set forth in this contract or agreement are unenforceable against the	X[31]					

[31] Referenced in another FAR Clause.

Table 18. Descriptions with Contract Language and Document Location

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL
	Government.						
Testing and Verification	The Contractor shall adhere to the processes described in the following references: DOD Cybersecurity T&E Guidebook v2, April 2018 and Addendum: Cybersecurity T&E of DoD Systems Hosted on Commercial Cloud Service Offerings			X			
Use of Subcontractors	The Contractor shall retain operational configuration and control of data repository systems used to process and store government data to include any or remote work. The Contractor shall not subcontract the operational configuration and control of any government data.			X			

Appendix B: Example Service Level Agreement (SLA) Checklist

Table 19. Example Service Level Agreement

	Yes	No	Comments
Pre - Onsite Assessment			
Prior to performing the assessment, you should protect yourself and your client by signing a BBG OGC approved Business Associate Agreement and having your client sign a letter authorizing the assessment including the external vulnerability test. The assessment must include everything from the layout of the office, locks and other methods to secure devices, and how visitors are managed should be observed. Was a BAA signed? Was a letter authorizing the assessment signed?			
Other Onsite Customers			
Was a list provided of the Cloud Service Provider's (CSP) major customers that they currently have onsite?			
Service Level Agreement			
The SLA requires that physical access controls—doors, locks, cabinets, cages, locking cables, and employee training—be implemented to protect health information. All Doors External and Internal? Locks (i.e., key, electronic, or both)? Locking Cabinets (i.e. internal to IT capability areas)? Locking Cages? Locking Cables? Documentation of Annual, Semi-Annual, Quarterly, Monthly, and any needed employee performance SKA training?			

Table 19. Example Service Level Agreement

	Yes	No	Comments
Is the nature and scope of the service provided (i.e., scope of the relationship, frequency, content and location of service to be provided) outlined?			
Does the SLA define the level of service and performance expected from a provider (for example, how that performance will be measured, and what enforcement mechanisms will be used to ensure the specified performance levels are achieved)?			
Was performance monitoring (i.e., includes clearly defined terms, definitions, performance measures/parameters and indicators) done?			
Were roles and responsibilities of all parties with respect to the SLA specified, and, at a minimum, were agency and cloud providers included?			
Was careful delineation between the responsibilities and relationships among the Federal agency, integrators, and the CSP done in order to effectively manage cloud services?			
Does the SLA define who is responsible for measuring SLA performance?			
Are reporting requirements (i.e., type, content and frequency of reporting; whether the performance is met; and reporting of incidents or events that may affect the service) outlined?			
A data-center is any third-party organization that hosts PII on servers or storage devices, no matter if owned by the client, a cloud service provider, or the data-center. The SLA requires data-centers to comply as BBG Business Associates because they ‘maintain’ data even if it is encrypted, or they cannot or do not access the data.			
Does the SLA cover the CSP-Prime and/or Sub-contracting on the access to data, the restrictions on sub-contracting, and clauses governing confidentiality of data? Require the provider to obtain individual confidentiality deeds from their			

Table 19. Example Service Level Agreement

	Yes	No	Comments
personnel? Restrict access to the agency's data to a limited set of the provider's personnel only? Restrict the type of provider information that is subject to confidentiality? For non-sensitive data, requirements to ensure the provider is aware of the level of confidentiality required and commits to protecting that data appropriately?			
Does the SLA define who is responsible for measuring SLA performance?			
Are reporting requirements (i.e., type, content and frequency of reporting; whether the performance is met; and reporting of incidents or events that may affect the service) outlined?			
A data-center is any third-party organization that hosts PII on servers or storage devices, no matter if owned by the client, a cloud service provider, or the data-center. The SLA requires data-centers to comply as BBG Business Associates because they 'maintain' data even if it is encrypted, or they cannot or do not access the data.			
Does the SLA cover the CSP-Prime and/or Sub-contracting on the access to data, the restrictions on sub-contracting, and clauses governing confidentiality of data? Require the provider to obtain individual confidentiality deeds from their personnel? Restrict access to the agency's data to a limited set of the provider's personnel only? Restrict the type of provider information that is subject to confidentiality? For non-sensitive data, requirements to ensure the provider is aware of the level of confidentiality required and commits to protecting that data appropriately?			

Table 19. Example Service Level Agreement

	Yes	No	Comments
Are business resumption and contingency requirements included?			
Are dispute resolution (i.e., protocol for resolving disputes and continuation of contracted service during disputes as well as the jurisdiction and rules under which disputes are to be settled) included?			
Is default termination and early exit by all parties provided for?			
Confidentiality and security (i.e., roles and responsibility, liability for losses in the event of breach of security/confidentiality and loss of data/misuse of data)?			
Ownership and access (i.e., ownership of assets generated, purchased or acquired during the outsourcing arrangements and your access to those assets)?			
What enforcement mechanisms are in the SLA (i.e., what penalties does a cloud service provider have for not meeting the SLA performance measures)?			
Overall Performance Measures			
Are Security controls considered to be shared, inherited, or dual controls?			
Are clear measures for performance defined by the contractor? Include which party is responsible for measuring performance. Examples of such measures would include: Level of service (e.g., service availability—duration the service is to be available to the agency). Capacity and capability of CSP (e.g., maximum number of users that can access the cloud at one time and ability of provider to expand services to more users). Response time (e.g., how quickly cloud service provider systems process a transaction entered by the customer, response time for responding to			

Table 19. Example Service Level Agreement

	Yes	No	Comments
service outages).			
Data location and Access (Regions, Availability Zones, and endpoints): Regions, Availability Zones, and endpoints are components of some CSP-secure global infrastructure. When you store data in a specific region, it is not replicated outside that region. Is it your responsibility to replicate data across regions, if your agency's needs require that? Or, do you need to require the CSP to do this as part of the SLA?			
Service-Specific Security Controls: Are service specific security implementation such as the Amazon Simple Storage Service (S3), security access permission settings, logging, event notification and/or encryption required? As a customer you may need to document service specific controls within their use of S3 in order to meet a specific security control objective related to employee records, PII and/or directory services related to training and education records.			
Optimized Network, Operating Systems (OS) and Application Controls: Are controls the customer may need to document in-order to meet specific control elements related to the use of Operating Systems and/or applications deployed within the SLA specifications?			
Specify how and when the agency has access to its own data and networks? This includes how data and networks are to be managed and maintained throughout the duration of the SLA and transitioned back to the agency in case of termination of service.			
Specify the following service management requirements: How the CSP will monitor performance and report results to the agency? When and how the agency, via an audit, is to confirm performance of the CSP?			

Table 19. Example Service Level Agreement

	Yes	No	Comments
Provide for disaster recovery and continuity of operations planning and testing (including how and when the CSP is to report such failures and outages to the agency). In addition, how will the provider remediate such situations and mitigate the following risks of such problems from recurring: Interruption to communications networks? Hardware or software failure? Power failure? Disaster (fire, storm, riot, etc.) that disables access to the service? The provider has a geographically separate disaster recovery site with seamless transition? The provider is able to operate in the event that mains power is disrupted (for example, use of Uninterruptible Power Supply and back-up generators)? Business continuity is a strict requirement and not subject to qualifiers such as 'reasonable efforts'? Business continuity and disaster recovery plan be submitted for comment and approval by the agency? Limiting the right for the provider to suspend their service for ‘force majeure’ reasons to circumstances where the business continuity and disaster recovery plan has been properly followed and implemented? Scheduled maintenance outages of provider systems do not occur during hours that the agency requires access and use of the system (a common problem if the service is provided from outside U.S. owing to time differences)?			
FISMA/FedRAMP Requirements Related to CSP Selection			
Please indicate which of the following will be actively involved in negotiating and reviewing the agency’s contract and ancillary SLA for cloud services:			

Table 19. Example Service Level Agreement

	Yes	No	Comments
Certified Cloud Broker? Accredited FedRAMP 3PAO? Contracting Officer/Procurement? Chief Information Officer? General Counsel? FOIA staff? Records Officer? Privacy Officer? e-Discovery Counsel or Representative? Cyber-security personnel?			
What is the process for developing the agency's needs criteria and evaluating the cloud provider proposal and post-award performance?			
Are the unique operational aspects of the cloud computing environment addressed in the acquisition plan required by FAR Part 7? In particular, in terms of the written acquisition plan format described in FAR Section 7.105, how are technical, schedule and cost risks addressed, and has any test and evaluation program and Government Furnished Information (GFI) to be considered?			
Based on market research conducted in accordance with FAR Part 10, does the acquisition plan contemplate use of a system integrator in addition to a Cloud Service Provider (CSP)? Will the CSP be a subcontractor to the system integrator, or will the CSP have a direct contractual relationship with the agency?			
Is there a clear statement in the contract for cloud services that all data is owned by the agency?			
Can the cloud provider access or use the agency's information in the cloud? (PS-1, PS-7, CM-5, SC-7)			

Table 19. Example Service Level Agreement

	Yes	No	Comments
How is the agency's data handled both at rest and in motion in the cloud? (SC-1, SC-28)			
Who has access to the agency's data, both in its live and backup state? (SI-1, SI-4)			
In the cloud, what geographic boundaries apply to data at rest and what boundaries are traversed by data in motion? (CM-1, CM-8) Where are the cloud servers that will store agency data physically located? (CM-1, CM-8, AC-4) Can the provider certify where the data is located at any one point in time?			
How will the cloud provider meet regulatory compliance requirements applicable to the Unified Security Gate (USG), [including but not limited to the Privacy Act, the Federal Information Management and Security Act (FISMA), The Paperwork Reduction Act, the Federal Records Act, the Freedom of Information Act (FOIA), the Trade Secrets Act and related guidance and authorities?			
What is the potential termination liability that would result from application of the contract clauses associated with FAR Part 49 Termination of Contracts? (SA-1, SA-2, SA-4, SA-12, SA-13)			
How is the migration of agency data upon contract termination or completion addressed? (SA-1, SA-4, SA-2, SA-12, SA-13)			
How is agency data destroyed? (e.g. upon request? Periodically?) (MP-1, MP-4) Methodology used? (e.g., remove data pointer or overwritten in accordance with USG security standards)			
How does the cloud provider segregate data? If encryption schemes are used have the design of those schemes been tested for efficacy?			
If the cloud provider or reseller agreement incorporates "URLs" into the terms, which policies and terms are being incorporated into the agreement? (URLs are not static and change over time)			

Table 19. Example Service Level Agreement

	Yes	No	Comments
What notice is provided to the agency if URLs/policies change? Remedies for agency if new policies or URLs are not acceptable?			
What remedies are being agreed to for breach or violations of the agreement? Litigation? Mediation? Waiver of right to sue? Are choice of law and jurisdiction provisions in the agreement appropriate? (e.g., has the agency unknowingly subjected itself and USG to the jurisdiction of a state or foreign court?)			
Is the agency indemnifying the cloud provider in violation of the Anti-Deficiency Act? What rights is the agency waiving, if any? What limitations of liability, whether direct or indirect, is the agency granting? How does the Force Majeure clause deal with the action of Federal agencies other than the customer agency?			
Can the agency manage content in the cloud with its own tools or only through contractor resources?			
How are upgrades and maintenance (hardware and software) handled? (e.g. who conducts these activities? How often? And how is the USG advised of findings?) (MA-1, MA-2, SA-7, SA-3)			
How are asset availability, compatibility, software updates and hardware refreshes addressed? What does the agreement say about estimated outage time the cloud provider foresees for standard hardware and software updates and the cloud provider's estimated response time should an emergency take the system off line?			
What responsibility does the cloud provider have for assuring proper patching and versioning control? What language is in the agreement specifically requiring the cloud provider to take on this responsibility?			

Table 19. Example Service Level Agreement

	Yes	No	Comments
Is there a discussion of how the cloud provider will continue to maintain or otherwise support the agency's data in a designated format to ensure that the data remains accessible/readable over the life of the data?			
Did the agency discuss with the cloud provider additional services that may be provided in the cloud, for example e- discovery tools?			
Does the contract support IPv6 as outlined per the FAR?			
If there is confidential statistical information at issue, does the agency agreement ensure the application of the provisions of the Confidential Information Protection and Statistical Efficiency Act of 2002 or similar statutes that protect confidential statistical information to the information in question?			
If there is confidential statistical information at issue, does the agency agreement contain provisions to ensure that either agency staff created and provided appropriate confidential statistical information training guidelines or actually delivered confidential statistical information training to the cloud providers?			
CSP and End User Agreements			
Before signing the contract, consider if the agency bound by the cloud provider's Terms of Service (TOS) provisions, in addition to the contract terms and conditions? If so, how do those terms deal with privacy, cybersecurity, data disclosure/access, etc.? Is the TOS document proposed by the CSP the standard for industry practice or is it proprietary to that offer or? Can the TOS proposed be revised through negotiation? Does the CSP need to sign Non-Disclosure Agreements (NDAs) to enforce acceptable CSP personnel behavior when dealing with Federal data?			

Table 19. Example Service Level Agreement

	Yes	No	Comments
e-Discovery Questions			
How does the agency or CSP halt the routine destruction of agency information in the cloud when a litigation hold has been implemented?			
Does the agency or the cloud provider's document retention/management plan apply to the agency's data stored in the cloud? Is it understood whose plan has priority in cases when they conflict?			
Is the metadata preserved when agency data is migrated into, out of, and within the cloud? (i.e., are transfers forensically sound)? Will the agency be able to search the data in the cloud by metadata field? For example, will the agency be able to batch search for all agency data in the cloud by original date created, file type, or author? Does the cloud provider ensure that metadata remains linked to records during data migration?			
Pursuant to the agreement, does the agency itself have the ability to search, retrieve, and review agency data in the cloud? Using the agency's own tools? Agency's e-discovery contractor's tools?			
What are the agency's file format export options for exporting agency data out of the cloud? What are the expenses associated with this process?			
Is the cloud provider or a third-party providing e-discovery services to the agency? What specific e-discovery services by the cloud provider are included in the contract? [NOTE: E-discovery services can include the process of managing, identifying/locating, preserving, collecting, processing, reviewing, and producing electronically stored information (ESI)]. What specific tools are being utilized for these e-discovery services? Will the cloud provider or third-party provide training on the e-discovery tools			

Table 19. Example Service Level Agreement

	Yes	No	Comments
offered? What project management resources will be available for the e-discovery services? Have the e-discovery services of the cloud provider or third- party been tested? If collection is one of the e-discovery services provided, is the collection method forensically sound? Can the agency modify the e-discovery protocol/process of the cloud service provider or third-party as warranted? How will e-discovery of data in the cloud be handled during user migration? Does the cloud provider have forensic or litigation experts available to answer questions and/or sign affidavits regarding the e-discovery services provide in the cloud? Will the cloud provider and third-party employees sign chain of custody affidavits to demonstrate the integrity of the ESI when needed for litigation purposes? If requested, will the cloud provider be able to supply the agency with audit trails, exception reports, and transaction logs? What if any additional charges will be required for e-discovery services discussed above?			
Does the contract require that the agency fund or otherwise support the cloud provider's response to a third party?			
Is the contract clear that the cloud provider and all associated subcontractors shall not release any agency information and/or data without written agency approval or about circumstances when such approval is not needed? Is the contract clear that the cloud provider will notify the agency within a mutually agreed upon timeframe when a request for agency information or data is received by the cloud provider or subcontractor? Who is the designated agency point of contact(s) for this notice?			

Table 19. Example Service Level Agreement

	Yes	No	Comments
If the agency desired to extract the data so that it can be loaded into a separate review platform, will work product from the cloud review platform be transferable to a separate review database?			
Will attorneys and staff have immediate access to review the data in the review platform if hosted by the cloud provider in the cloud? Is there 24/7 access to the review platform? Can approved, non-agency personnel (i.e. other agencies or contractors) access the review platform in the cloud?			
Faxing used to be paper documents being sent and paper documents received. Today faxes can be originated or received electronically, with images stored locally or with vendors.			
Cybersecurity Questions			
Will the service provider be outsourcing any of the SLA requirements; activities, functions or operations?			
Does the contract include provisions to meet all FedRAMP requirements?			
Who is responsible for the security of the data that resides at the CSP locations within the U.S.?			
Is there a prohibition on the provider transmitting data outside of the U.S. without the prior approval of the agency?			
Are Network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network? Note: These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services.[32]			

[32] NIST SP 800-53 rev.3 FedRAMP Control: CM-2

Table 19. Example Service Level Agreement

	Yes	No	Comments
Has the CSP strategically placed a limited number of access points to the cloud to allow for a more comprehensive monitoring of inbound and outbound communications and network traffic?			
Has the level of security and encryption to be applied to agency data held and transmitted by the provider been verified and tested?			
What additional security controls will be utilized above and beyond those provided by the CSP?			
Is the CSP 3rd party certified/accredited to the following standards applicable to your operations? ISO/IEC 27001:2013: Information technology -- Security techniques -- Information security management systems – Requirements ISACA COBIT 5 Standards for Attestation Engagements (SSAE) No. 16 ISO/IEC 31000:2009 (E) Capability Maturity Model® Integration (CMMI®) ISO/IEC 20000-1:2011 - Information technology – Services Management Systems Standard ISO/IEC 24762:2008 Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services			
What Accreditation Body's Certification Body issued the certification, when (i.e., year) and what was the "scope" of the audit/certification?			
An External Firewall is a device used to protect a network from external attacks. Firewall functionality may be built into some routers. In those cases, the router models should be investigated for additional functionality. Firewalls include Intrusion Detection and Intrusion Prevention features. Many also offer network perimeter protection against viruses and other malware.			

Table 19. Example Service Level Agreement

	Yes	No	Comments
Deploy hardened operating systems – systems software and firewalls should be configured to the highest security settings consistent with the level of protection required, keeping abreast of updates, patches and enhancements recommended by system vendors; change all default passwords for new systems immediately upon installation.			
Install firewalls between internal and external networks as well as between geographically separate sites.			
Install intrusion detection-prevention devices (including denial-of-service security appliances where appropriate).			
Develop built-in redundancies for single point of failure which can bring down the entire network.			
Perform application security review using a combination of source code review, stress loading and exception testing to identify insecure coding techniques and systems vulnerabilities.			
Engage independent security specialists to assess the strengths and weaknesses of internet facing applications, systems and networks before each initial implementation, and at least annually thereafter, preferably without forewarning to internal staff.			
Conduct penetration testing at least annually. If yes, provide: Date of last penetration test: _____ (DD/MM/YY) Name of firm that conducted the test: Please attach a copy of the penetration test report.			

Table 19. Example Service Level Agreement

	Yes	No	Comments
Establish network surveillance and security monitoring procedures with the use of network scanners, intrusion detectors and security alerts.			
Implement anti-virus software and apply updates regularly.			
Conduct regular system and network configurations review and data integrity testing.			
Maintain access security logs and audit trails.			
Analyze security logs for suspicious traffic and intrusion attempts.			
Establish an incident management and response plan.			
Test the predetermined response plan relating to security incidents.			
Install network analyzers which can assist in determining the nature of an attack and help in containing such an attack.			
Develop and maintain a recovery strategy and business continuity plan based on total information technology, operational and business needs.			
Maintain a rapid recovery capability.			
Conduct security awareness education and programs.			
Require frequent ICT audits to be conducted by security professionals or internal auditors who have the requisite skills.			
Consider taking insurance cover for various insurable risks, including recovery and restitution costs.			
Provide separate physical/logical environments for systems development, testing, staging and production; connect only the production environment to the internet.			
Implement a multi-tier application architecture which differentiates session control, presentation logic, server-side input validation, business logic and			

Table 19. Example Service Level Agreement

	Yes	No	Comments
database access.			
Implement two-factor authentication at login for all types of online systems, such as internet banking, online trading platforms, insurance portals for policyholders as well as a specific OTP or digital signature for each value transaction above a specified amount selectable by the customer or predetermined by your organization.			
Deploy strong cryptography and end-to-end application layer encryption to protect customer PINs, user passwords and other sensitive data in networks and in storage.			
Encrypt customer account and transaction data which is transmitted, transported, delivered or couriered to external parties or other locations, taking into account all intermediate junctures and transit points from source to destination.			
On-site Wireless networks are often overlooked as a security vulnerability. While a hacker or former employee may not be able to enter a facility to plug into a network, they may be able to park outside or come close enough to get wireless access.			
Deploy strong user authentication in wireless local area networks and protect sensitive data with strong encryption and integrity controls.			
Physical Security Questions			

Table 19. Example Service Level Agreement

	Yes	No	Comments
Has there been a site physical security assessment of every CSP site your information will migrate across which typically involves interviews with key staff, documentation review, and an on-site visit to assess appropriate physical and environmental controls for safeguarding computing resources? If so, Year and Date, and what entity conducted the assessment? Political (e.g., cross-border conflict, political unrest etc.) Country / socioeconomic Infrastructure / security / terrorism Environmental (i.e. earthquakes, typhoons, floods) Legal			
Are Data centers staffed 24x7 by trained security guards, and access is authorized strictly on a least privileged basis?			
Are Environmental systems designed to minimize the impact of disruptions to operations?			
Are multiple geographic regions and Availability Zones allowing you to remain resilient in the face of most failure modes, including natural disasters or system failures?			

Table 19. Example Service Level Agreement

	Yes	No	Comments
Are the following physical and environmental controls available at the data center? Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Physical access controls such as locked doors, access cards, biometrics access, etc. Proper approval sought for visitors to gain access to the data center. Visitors escorted by staff Records of visitor's activities Systems and network equipment’s locked up in cabinet Uninterruptible power supply Air conditioning system Temperature sensor Fire detector Smoke detector Water sprinkler (dry-piped or wet-piped) FM200 or other fire suppression system Raised floor CCTV Water leakage detection system Fire extinguisher			
Does the SLA define the level of access security protocols to be implemented by the provider to defeat unauthorized attempts to access the data by third parties, provider personnel and other customers of the			

Table 19. Example Service Level Agreement

	Yes	No	Comments
provider?			
What happens when material infringing on the intellectual property rights of the USG or others is located in a cloud system deployed by a cloud provider for the benefit of the USG? What level of indemnity and supporting insurance and/or capital will be provided by the cloud provider to the USG? What access to cloud provider intellectual property rights will the USG need to address various issues, particularly law enforcement investigations and audits?			
What happens when USG data is stored or transported in non-bannered environments and devices, particularly if those environments also contain data not belonging to the USG?			
Where physical media is damaged and replaced, does the SLA or the provider have established requirements for the sanitization or deletion of data in the damaged media?			
Does the SLA or the provider cover the way in which separate packages of data are to be stored – for example, it may be important to avoid the provider aggregating separate packages on the same hardware (as such aggregation may increase the sensitivity of data or risks to security of the information)?			
Can the vendor access or use the information in aggregate?			
Does the SLA or the provider cover the way in which storage of data on specified hardware that is unique to the agency so that there can be security precautions set up between the hardware storing the agency's information and other hardware held by the provide?			
What security guidelines apply to operations of various cloud components and how are they measured for compliance? (SA-1, CA-2, SA-4, SA-13)			
Was there an assessment by the agency or cloud provider of how server and telephony locations may impact access and security of the data? (AC-1, AC-16, SA-4)			

Table 19. Example Service Level Agreement

	Yes	No	Comments
Privacy Questions			
If cloud services host “privacy data,” has the agency cybersecurity staff adequately identify potential privacy risks and responsibilities and address these needs in the contract?			
E-mail is a common tool used for business and personal communications. ePHI should only be sent within, or attached to, an e-mail message within a secure network or if the service complies with HIPAA and has signed a Business Associate Agreement.			
When implementing a cloud solution, did the agency consider whether any personally identifiable information (PII) would be involved?			
Did the agency consider whether any other categories of personal information, such as those protected by special privacy legislation and regulations like protected health information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, would be involved?			
If there is PII at issue, did the agency assess whether the Privacy Act of 1974 applied to the PII in question? If so, did the agency ensure that the agreement included mandatory FAR language on operating Privacy Act systems of records?			
If there is PII at issue, did the agency conduct a Privacy Impact Assessment in accordance with section 208 of the E- Government Act of 2002 and OMB Memorandum M-03-22?			
If there is PII at issue, does the agreement provide instruction and requirements on what to do in the event of a breach or unintentional release of PII?			
If there is PII at issue, did the agency make any arrangements to ensure that either agency staff created appropriate PII training guidelines or actually delivered PII training to the cloud providers?			
If there is PII at issue, does the agency agreement provide instruction and requirements on what to do in the event of any request for disclosure, subpoena, or other judicial process seeking access to the records which			

Table 19. Example Service Level Agreement

	Yes	No	Comments
may include USG PII?			
If there is PII at issue, does the agency agreement limit uses strictly to support the agency and prohibit uses for other purposes?			
If there is PII at issue, does the agency agreement provide instruction and requirements on terminating storage and deleting data upon expiration of the agreement term and option extensions?			
If there is PII at issue, does the agency agreement specify whether the data servers, including redundant servers, may be located outside the United States?			
E-Discovery			
Federal agencies must ensure that all data stored in a CSP environment is available for legal discovery by allowing all data to be located, preserved, collected, processed, reviewed, and produced.			
Freedom of Information Act (FOIA) Questions			
Does the agreement address whether the CSP supports the agency's FOIA process? If the agency has a centralized FOIA searching process, does the CSP facilitate this searching capability? If the agency requires each individual who may have responsive records to conduct their own search, does the CSP allow an individual to search and retrieve their own records? If the agency has FOIA professionals conduct searches for ESI, does the CSP provide appropriate access for FOIA professionals to agency custodians' records systems? Are any time constraints imposed by FOIA taken into account in the agreements, so that the FOIA office has adequate time to review the documents?			

Table 19. Example Service Level Agreement

	Yes	No	Comments
Are there processes in place so that cloud provider adequately communicates with the FOIA office as needed?			
Pursuant to the agreement, does the agency itself have the ability to search, retrieve, and review agency data in the cloud? Using the agency's own tools?			
What are the agency's file format export options for exporting agency data out of the cloud? What are the expenses associated with this process?			
Can approved, non-agency personnel (i.e. attorneys or contractors) access the review platform in the cloud?			
Recordkeeping Questions			
Agencies must ensure CSPs understand and assist Federal agencies in compliance with the Federal Records Act (FRA) and obligations under this law.			
Is the information that will be moved to the cloud-based system adequately scheduled as a Federal record?			
Does the cloud provider allow the agency to destroy (truly delete) all copies or renditions of records from the cloud when appropriate?			
Does the cloud provider allow the agency to implement records disposition policies across categories of records?			
Does the cloud provider have a process that allows the agency to capture records that are appropriate for permanent preservation and transfer to NARA in accordance with NARA regulations as they may exist at the time of the transfer/accessioning to NARA, including file format?			
Is the cloud provider using non-propriety file formats so that the data will remain useful outside of the system in which it was created?			
Is the cloud provider capable of retaining the integrity of the files for the duration in which the agency's records schedules contemplate them being kept?			

Table 19. Example Service Level Agreement

	Yes	No	Comments
Can the cloud provider migrate records to an agency's in-house servers on demand, in the event it is necessary to do so?			
If the agreement is for infrastructure as a service, has the agency considered the kind of record material which may be lost if the cloud provider were to change?			
Did the agency consider if there were special substantive categories of records, such as vital records, being moved to the cloud for which increased records management attention is needed?			
Auditing			
Are the following rights of the agency covered in SLA: Restricting the locations/countries in which agency data may be held Rights to audit the provider's compliance with the agreement including rights of access to the provider's premises where relevant records and agency data is being held Audit rights for the agency (or its nominee), the Auditor, DoS OIG-Inspector General and appointed agency OCIO staff A right for the agency to appoint a commercial auditor as its nominee (as this allows the agency to appoint an auditor in the same location as the provider's data center to save costs and ensure compliance with relevant jurisdictional laws) Where technically available, the right for the agency to remotely monitor access to its data			
Cancelling the Contract			
Does the SLA detail, how do we cancel the contract and migrate the information?			
How are data and media destroyed?			

Table 19. Example Service Level Agreement

	Yes	No	Comments
How do you get the replacement CSP to assist in the cost of data migration?			
Exception Criteria Performance Measures			
Are there exceptions criteria when the provider's performance measures do not apply (e.g., during scheduled maintenance or updates)?			
Security Metrics Performance Measures			
Specify metrics and verification testing in the lines below that the cloud provider must meet in order to show it is meeting the agency's security performance requirements for protecting data [e.g., clearly define who has access to the data (both in its live state and when backups are made], and the protections in place to protect the agency's data. Specifies performance requirements and attributes defining how and when the cloud service provider is to notify the agency when security requirements are not being met (e.g., when there is a data breach). A requirement for the provider to notify the agency immediately in the event of security incidents or intrusions, or requests from foreign government agencies for access to the data, to enable the agency to manage these events proactively.			

Table 19. Example Service Level Agreement

	Yes	No	Comments
Consequences for Non-Compliance with Performance Measures			
Unmet Performance Measures	Enforceable Consequences (Penalties)		
IT Contingency and Incident Response Planning			
Questions	Comments		
What's the current date on the IT Contingency Plan(s)? (ref. FISMA CP-1-10)			
When was the last Business Impact Analysis (BIA) and Risk/Vulnerability Analysis?			
What's the current date on the IT Contingency Plan(s) supporting Incident Response Plan(s)?			
Are incident roles and responsibilities defined?			
Who is responsible for incident response planning?			
Are there clear lines of reporting related to incidents?			
Are incident types defined?			

Table 19. Example Service Level Agreement

	Yes	No	Comments
When was the Incident Response Plan last reviewed and who approved it? And how often are they reviewed?			
How does incident response fit into the overall Information Security Program?			
Does the Incident Response Plan include a document history to record changes?			
Who is responsible for updating the plan with revisions?			
Were any revisions made after the last testing exercise?			
How do you prepare for incidents?			
Who should agency customers call if they suspect an incident?			
Is there an incident hotline or phone number published where customers can see it?			
What capability do you have to detect incidents?			
If you suspect an incident how do you verify if it really is an incident?			
What methods do you use to analyze confirmed incidents?			
What methods do you use to contain incidents?			
What methods do you use to eradicate incidents?			
What is your process for determining that the system has recovered from the incident?			

Table 19. Example Service Level Agreement

	Yes	No	Comments
Which incident handling activities are coordinated with contingency planning activities?			
How does the coordination take place?			
Which incident handling activities are coordinated with contingency planning activities?			
Who maintains archives of lessons learned regarding incidents?			
How do you determine which incidents require a lessons learned report?			
How soon after an incident is closed will the lessons learned report be published?			
Who is responsible for integrating lessons learned into procedures, training, and test/exercises?			
What personnel security requirements are required of individuals who perform incident handling?			
Is there any sort of online workflow tool used for managing incidents?			
Are there any automated alerts related to incidents?			
Are there any automated programs, scripts, or applications that look for incidents or suspicious activities?			
What mechanism is used to record and track information about incidents?			
Do you have an incident reporting and tracking form?			
Is the incident reporting form online on your intranet? Where?			

Table 19. Example Service Level Agreement

	Yes	No	Comments
Is the incident reporting form a .pdf file?			
Can you insert a blank copy of the incident reporting form?			
Is there a place on the incident reporting form to indicate if PII4 has been compromised?			
Who is responsible for ensuring that incidents are documented internally?			
Who will be the FedRAMP point of contact for incidents?			
Who will be the point of contact for customer agencies			
Is there a flow chart to show how decisions about incident escalation are made?			
What notification timeframes are built into your incident reporting process?			
Do your reporting timeframes line up with Table J-1 in NIST SP 800-61, Revision 1?			
Who will ensure that incident reporting timeframes are adhered to?			
Who at your company determines if law enforcement should be notified?			
What decisions need to be made before law enforcement is notified?			
Do you have the contact information for all of your agency customers?			
Is there an online Incident Reporting Form that is available to your staff?			

Table 19. Example Service Level Agreement

	Yes	No	Comments
Is there an online Incident Reporting Form that is available to your customers?			
Are there any apps for Incident Reporting?			
Have you identified incident response experts within your own organization?			
Do you track how many incidents occur each month/year?			
Do you track what types of incidents are most prevalent?			
Do you track the average time it takes to close an incident?			
On-Site Chief Information Security Officer (CISO)			
Name of the on-site Chief Information Security Officer or individuals in-charge 24/7 who will act as a central point of contact:			
Name	Phone Number		

Table 20. CSP and End-User Agreements

CSP and End-User Agreements	Yes	No	Public, Private, Hybrid, Community
Have you established the necessary agency required “Terms of Service and all CSP/customer required agreements” needed to be integrated fully into cloud service providers contracts?			

Table 21. Type of Cloud Service

Type of Cloud Service	Yes	No	Public, Private, Hybrid, Community
Applications as a Service (AaaS)			
Business Process as a Service (BPasS)			
Infrastructure as a Service (IaaS)			
Platform as a Service (PaaS)			
Software as a Service (SaaS)			
Massively Scaled Software as a Service (MSSaaS)			

Appendix C: Examples of Commercial Cloud Acquisition Scenarios

Federal agencies face a common set of situations when deciding to acquire cloud solutions. This is the basis for the scenario-based approach that Appendix C takes. The most common instructive situations are reflected in Figure 18, Visual Scenario Reference below. Usually, the situation and needs of an agency can be organized into four categories of services:

1. Inventory Assessment. A formal, documented, and current record of applications and IT assets with corresponding descriptive attributes.

2. Application Preparation. Applications that will be moved into the cloud are refactored, modernized, and certified to run in a cloud.

3. Migration Support. A determination regarding how the migration will be performed - whether internal agency resources will perform the migration to the cloud or this work will be sourced.

4. CSP. The agency will obtain the core cloud computing services (e.g., hosting) from the cloud service provider (CSP).

Once an agency determines the results of these factors, an agency stakeholder can immediately identify the scenario that intersects most often with the answers to the knowledge questions of the agency. They can then turn to that section of the Guidebook to begin preparing for and acquiring the needed services. As the Guidebook is not exhaustive, program managers must be willing to assess intent, generally apply criteria, and make decisions when using the Guidebook. The decision regarding the proximity of the situation of the agency to these factors results in valuable and actionable information allowing them to get their acquisition started.

To Use this Appendix

Evaluate the situation of your agency relative to the four factors above and reflected as Services Sought headers in the Visual Scenario Reference below. Assess your needs by column starting with “Inventory Assessment.” Mark whether you “Need This” or “Have This.” Move to the next column and make the same assessment for “Application Preparation.” Make the same assessment in the final two columns. Identify the row that has the most “Need This” Marks. Your agency should run the scenario that corresponds to this row.

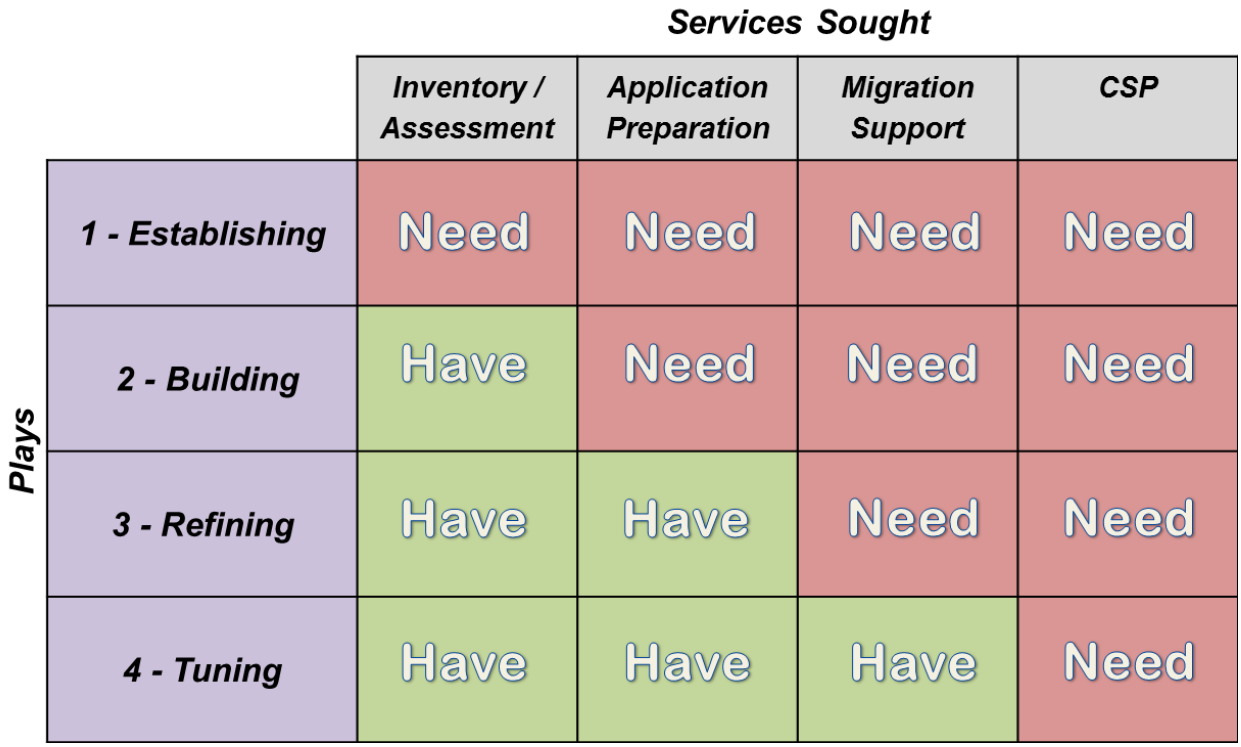


Figure 19. Visual Scenario Reference

Scenario Structure

As mentioned before, the Appendix is a scenario-based document. Once the scenario is identified, consider the scenario components. The scenario component definitions are defined below.

Initial Conditions. This is a composite situation of factors that have been brought together in a rationalized set of information to better communicate and guide cloud elements that stakeholders should consider when planning a cloud acquisition. All of the elements in the scenario influence applicability of the scenario, but the more directly the scenario information is related to the factors of consideration in the Visual Scenario Reference the more strongly agencies should consider them when making decisions.

Additional Assumptions (to Scenario above)**.** These assumptions are provided to further refine agency assessment and decision-making.

Checklist. This is a checklist of the most important items that should be considered as they contribute to the success of a cloud acquisition.

Key Questions. The list of key questions prompts topics and guidelines that are likely to increase success of a cloud acquisition. The information here expands on key information and topics in the Checklist and is broader in scope to provide a line of thinking that eases acquisition and increases likelihood for success.

Discussion. This is the most detailed exploration of the scenario, its components for consideration, and supporting elements. It is a customized discussion of the scenario and deals in depth with the key points, risk management, and benefit assessment. The focus is on developing an improved understanding of the services being procured to drive solicitation structure and content to enhance overall project success.

Scenario

The following subsections present each scenario in detail and provide the relevant discussion, checklists, and assumptions that accompany each scenario.

Scenario 1: Establishing Cloud

	Services Sought			
	Inventory / Assessment	***Application Preparation***	***Migration Support***	***CSP***
1 - Establishing	Need	Need	Need	Need

Figure 20. Visual Scenario Reference, Establishing Cloud

Initial Conditions

- Your solution to data center consolidation is an Infrastructure-as-a-Service (IaaS) solution.
- Your plan is to complete movement onto the solution in phases. This project is phase 1 and the goal is to move key support infrastructure and four related mission critical applications into the cloud.
- Systems development efforts have been fragmented over time and recent centralized documentation efforts highlight inconsistent standards and coverage gaps.
- The targeted systems for migration have differing legacy architectures and current modernization plans are not comprehensive and aligned with current goals.
- You are in a small agency (10,000 employees).
- You have client-server based, premise solutions for the majority of your mission services.
- Many of your current infrastructure services are virtualized.

Additional Assumptions

Agency staff and support contractors have application support expertise, but limited expertise or bandwidth for executing application upgrade and migration tasks.

Single acquisition and any existing support contracts will be only minimally leveraged.

Checklist

- ❑ Inventory and definition of both existing infrastructure services and infrastructure services to be deployed as part of the contract.
- ❑ Current enterprise and solution architecture documentation.

- ❑ Current application definition list.
- ❑ Application reconciliation plan.
- ❑ Network architecture and connectivity – Trusted Internet Connection (TIC) compliance is met and required common services for integrations are available within required service levels.
- ❑ Organizational knowledge development plan.
- ❑ Documented support plan during migration.
- ❑ Thorough market research for system integrators (SI).

Key Questions

- Will your current service level definitions accommodate this delivery plan?
- Is your security breach and notification plan thorough, compliant and resilient?
- Will you need a headcount surge plan to support cutover periods during migration?
- Are you planning for changes to your disaster recovery (DR) and continuity of operations (COOP) plans?
- Are your administration rights, delegation, and credential issuing plans sound?
- Do you have a full understanding of affected software licensing that will move to the cloud?
- What mission critical services, if any, will you continue to deliver on-premise? Are there services you plan to source differently than on-premise or from the IaaS CSP?
- Have you considered differences in communications with users under the new service delivery plan?
- Do you have a requirements definition that clearly defines duties of the provider relative to duties of the government?
- Are the stakeholders in all key areas at the same industry knowledge level for cloud?

Discussion

Inventory and Assessment

An accurate and complete inventory and assessment of all IT system assets is important for IT management and is critical for successfully migrating those assets to the cloud. A big-bang transition involving all systems at once is seldom financially feasible and risk warranted. Therefore, fully documented current state information, along with change management processes to keep them maintained, is key baseline information to include in future acquisitions for later migration phases.

There are three main elements within an inventory and assessment phase to provide a foundation and roadmap for modernizing the IT enterprise. The first is the inventory, gathered from both automated scans and stakeholders. This inventory documents all IT assets and provides both a physical and a logical organization to those assets such as by application system, environment (dev, production, etc.), circuit, physical location, and organizational control. The next element is the application rationalization which documents business functions and system integrations. The outputs are specific modernization plans and recommendations including eliminating duplicative systems by merging application functions, terminating legacy applications with minimal business value, and complete application re-engineering when warranted. The third element is the actual migration planning which is often constrained by budgetary considerations and necessarily considers risk assessments for prioritization. GSA developed at the request of OMB, and in collaboration with industry partners, a set of statement of objectives (SOO) templates for agency use in acquiring cloud

migration services.[33]

Goals for the inventory and assessment work, and the contractor deliverables to drive the milestones, include 1) a complete inventory and assessment to establish a baseline for later migration implementation phases and 2) producing a rationalization and modernization plan for the targeted support infrastructure and four mission critical applications. Although a variety of existing agency situations and goal states may exist for this type of work, this aspect of the project is typically best serviced with firm fixed price (FFP) type contracts.

Application Preparation

The existing agency experience with virtualization for its current server assets is a benefit in capacity planning and right-sizing virtual machine (VM) resources in the target environment. Providing these as-is details in the solicitation enhances contractor understanding of the overall effort but is not as informative in developing levels of effort for application preparation as the outputs from their inventory and assessment phase. The scenario indicates a prevalence of client-server architecture that generally does not indicate a fully service oriented, cloud-ready architecture. The agency can reasonably expect various levels of application refactoring to be required in the move to the cloud. The detailed application assessment process presents the opportunity to make appropriate investments in modernization such as enhancing business value, improving security to latest standards, rationalizing and consolidating data stores, and reducing complexity while migrating to a scalable platform.

High level goals for the to-be state for the targeted support infrastructure and the four missions related applications are necessary to guide the contractor. To the extent that agency enterprise architecture standards are already developed, these need to be a part of the referenced standards in the acquisition documentation. Given the minimal cloud adoption of the agency, these standards likely do not reflect your current future state. At the very least the standards will be lacking considerable details that will be developed during this project. This type of documentation and standards maintenance should be built into a strong governance and change management process at the agency. Whether these structures and guidance are complete at the outset, guidelines need to be provided in the acquisition to ensure agency IT service agility and responsiveness are achieved and enhanced.

The challenge in this scenario is that at the time of acquisition, without reliable and comprehensive inventory and application dependency information, bidding contractors will have a difficult time making accurate estimates for the scope of application modernization efforts to undertake. Contracting approaches for managing this work includes using T&M contract line item numbers (CLINs) for this part of the work and further requesting multiple options with trade-offs be produced in the plans prepared for the rationalization and modernization effort. Alternatively, one or more optional CLINs could be used to selectively undertake recommendations arising from the assessment activities completed earlier.

Migration Support

The agency mission will require significant resources to plan and execute the migration of these related systems.

[33] Cloud migration services SOO templates https://gsa.gov/portal/content/141191

Required activities include project management and stakeholder coordination support, in addition to the technical expertise for planning the cloud environment, configuration, testing, building and scheduling the cutover plan. Program Managers should expect resources to ramp up and down for this part of the work since minimal resources can be effectively deployed until the inventory & assessment phase is complete. Further, anticipate scheduling flexibility for various overall project milestones since key decisions on technical approaches will be based on the outputs of the assessment, planning, and application development work completed earlier.

Network architecture and agency circuit capacity for the network traffic between agency premises and the CSP is a key planning element. Patterns vary widely for network traffic and utilization by applications based on the variety of types, number, and logical location (public, internal agency, trusted systems, etc.) of users and systems connecting as well as the amount of data transferred. The inventory and assessment phase considers these issues and can even indicate a scope change to the targeted migrated systems based on this information. Prior market research should inform whether a dedicated circuit to the CSP is warranted as part of the overall project. Anticipate coordinating appropriate changes to the existing agency telecom and circuit contract as the approach is determined. At a minimum, plan for the acquisition to specify development of networking architectures to ensure sufficient bandwidth and a TIC-compliant solution.[34] Note there can be challenges with some cloud-exclusive type architectures in meeting monitoring requirements contained in TIC, but it does remain a Federal requirement.

To the extent possible within this project and acquisition, executing a phased migration with the key support infrastructure moving first will lower risk more than performing a complete cutover of all targeted applications at once. Subsequently, migration of the four targeted applications individually may limit the scope of potential related mission delivery problems. Since moving a significant portion of IT services is contemplated in this project, a phased approach to effectively test networking, latency, and overall service performance is useful in potentially limiting the scope of affected systems with each change. Consider moving key support infrastructure first or early in the process to shed light on undocumented dependencies within the systems and applications that are not in scope for migration in this phase. When it is architecturally feasible to do so, move individual components within an application in stages to mitigate cutover risk in the cases. Effective testing of production systems in new environments can be challenging and, given the mission critical nature of the targeted applications, these strategies may prove effective.

CSP

CSP specific requirements won't likely be numerous in a scenario where there is little agency cloud footprint and itis the first significant foray for the agency into cloud. DR and COOP requirements are best treated at the application level versus viewing the CSP as a traditional datacenter and layering on outmoded legacy backup requirements. The goal is a transition to the cloud and an associated operational transformation to an efficient service-oriented posture. Include a geographic diversity requirement; it is easily met by most CSP. Granted, not all (and perhaps even few) typical Federal agency applications will ever be re-engineered into fully next generation cloud-designed applications that are stateless works of resiliency, but it still makes sense to position the organization to leverage this potential where appropriate. Focus CSP-specific specifications on items such as average resource deployment times, resource configuration

[34] https://www.dhs.gov/trusted-internet-connections

requirements (e.g. VM's with 16 cores), resource performance (e.g. network and block storage IOPS), and functional characteristics such as fully API-enabled access to all capabilities.

This scenario contemplates migration of four mission critical applications. Assign application availability SLA's to the contractor layering managed services above the CSP and not directly with the CSP hosting the resources. The implementation path the contractor chooses to achieve those service level objectives (SLOs) will vary based on the particulars of the application architecture. Specifying those goals influences the approaches taken during the application preparation phases to enhance application resiliency. Specify Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) at the application level (or standardized across groups of applications).

Additionally, the Federal Information Security Management Act (FISMA) security categorization of the applications to be hosted is a key requirement for defining the CSPs that can be leveraged by contractors. PMs should plan for proactive management and processes to monitor CSP resource consumption by requiring reporting and providing mechanisms for managing and periodically reviewing consumption. Contracting flexibility can be provided by employing optional contract line item numbers (CLINs) within appropriate resource categories to accommodate future growth.

Contract Vehicle Options

Projects of this advanced complexity with a soup to nuts scope need a full range of IT professional services to support the entire range of inventory and assessment, application development, and migration support functions that are required. Projects with these labor requirements and multi-phase executions are typically most easily accommodated by the IT solutions based GWACs such as GSA Alliant and NITAAC CIO-SP3 as they have the flexibility and capability for such an enterprise lift. Agency specific IT solutions contracts such as DHS Eagle II and VA's T4NG may be similarly suitable for those ordering activities eligible to use them. Cloud focused contracts that support the full range of services required such as DOI's Foundation Cloud Hosting Services (FCHS) can be appropriate on a government-wide basis and Army's ACCENT contract is a candidate as well for Army mission owners. Although there is no individual requirement outside the scope, the multi-phase approach and broad range of requirements may render Schedule 70 an imperfect fit. The large delivery-order based contracts such as NASA SEWP and NITAAC CIO-CS would not be suitable due to the overall project emphasis on services including the analysis, assessment, and software development aspects of this project.

Scenario 2: Building Cloud

	Services Sought			
	Inventory / Assessment	*Application Preparation*	*Migration Support*	*CSP*
2 - Building	Have	Need	Need	Need

Figure 21.Visual Scenario Reference, Building Cloud

Initial Conditions

- Management has asked you to move your largest line of business to the cloud.
- Your agency recently completed an IT systems application inventory and assessment as part of a successful governance process remediation effort.
- Your agency has put a single business support application in the cloud last year.
- You are from a medium sized component agency (25,000 employees) within a cabinet level department.
- You worked for a cloud provider before joining your current agency.
- Most agree, your CIO shop is stretched to capacity.

Additional Assumptions

- Some application re-engineering within this largest line of business (LOB) application will be required prior to migrating to cloud.

Checklist

- ❑ Current enterprise and solution architecture documentation.
- ❑ Application reconciliation contract or internal work plan.
- ❑ Organizational knowledge development plan.
- ❑ Post-migration application support strategy.
- ❑ Network architecture and connectivity – TIC compliance is met and required common services for integrations are available within required service levels.
- ❑ Cost goals that reflect what is more expensive and what is less expensive when deploying cloud services.

Key Questions

- What is the condition of your enterprise architecture blueprints? Are they good enough to facilitate migration of the LOB app to a CSP?
- Have you decided what identity management approaches are acceptable and desirable?
- Do you have a comprehensive set of service level agreement (SLA) requirements? Does it include acceptable application performance metrics?
- Do you have a “consumption-to-cost” management and adjustment mechanism?
- Is governance in place?
- Can you discuss your strategy for cloud sourcing? Do you have a roadmap?
- Are the stakeholders in all key areas at the same industry knowledge level for cloud?
- Is your security breach and notification plan thorough, compliant, and resilient?
- Will your current service level definitions accommodate this delivery plan?

Discussion

Application Preparation

With the target project consisting of your largest LOB, risk is elevated for your cloud migration. By leveraging features of cloud computing, you are taking the opportunity to modernize your critical application to improve reliability and lower future maintenance burdens. Careful application preparation is needed to ensure current documentation, improve the security posture, leverage modern architecture and interface capabilities, and enhance testing and maintenance efficiency.

However, this significant project builds on the prior cloud experience. The prior business support application migration contemplated some network topology and systems integration concerns. Consider complying with processes defined at the department level. When these considerations are well executed they can provide useful elements that can be leveraged by the component agency. Contracting for IT projects of this type always requires detailed and comprehensive system descriptions of the as-is state and detailed objectives for the to-be state.

As an IT system inventory and assessment has been completed, much of the as-is documentation for this system / line-of-business has been completed and remains current. The scope of that initial effort may have outlined some modernization paths for this application suite. In the more likely scenario that it did not, your current project will need to anticipate some uncertainty in the implemented approach to its preparation for the cloud. Given the assumption of a single acquisition, you'll be asking vendors for an end-to-end solution approach. This can result in sub-optimal outcomes if various vendors propose different approaches to the project sections with no vendor proposing what might be the best approach for each project section. Early contractor engagement during market research and especially the use of RFI's can be very valuable in providing input to framing the project and the solicitation to ensure that the organization's goals are met.

The to-be state after application refactoring must be consistent with your existing component agency enterprise architecture, platform, and security standards and further require inclusion of the department-wide versions of those same documents. All of these documents need to be referenced in the solicitation and some judgements will need to be made if there are conflicts between the documents or if they are undergoing resolution processes. If exceptions to such standards have been made for this project, such as a particular legacy system component to be replaced separately, those should be clearly noted as well.

Multiple contracting approaches are possible with complex multiple phase projects. Separate CLINs can be created for each phase and these can be broken down further within a phase. Hybrid contract types with optional CLINs mixing FFP and T&M (or just Labor Hour) provide tremendous flexibility to ensure successful project execution.

Migration Support

Transition to the new cloud hosting environment requires agency staff resources and existing contractor application support resources. In addition to these resources, anticipate needing transition related support activities including project management for the planning, implementation, cutover, and legacy shutdown activities for the application. The important theme for both your project, and especially the related solicitation, is to be clear and thorough in identifying the roles and responsibilities of existing stakeholders and those to be undertaken by your new contractor. As the comprehensiveness of the descriptions of the as-is and to-be states increases within the solicitation, the ability to use FFP contracting for the migration work will also increase.

CSP

The overall scope of the line of business application being migrated may consist of many subsystems creating a large footprint of VM's, storage, and bandwidth consumed by the aggregated whole. This initial resource footprint will be further multiplied when factoring in the various environment instances required for a full development lifecycle such as for development, integration, quality assurance (QA), and production environments. Pricing the CSP is a challenge for the contractor. Compounding the contractor's problem in pricing such services will be the phased approach of the

project and potential significant unknowns in the application modernization and preparation phase that will impact resource consumption while seeking to maintain performance characteristics.

Plan for proactive management of CSP resource consumption by requiring estimates and providing mechanisms for managing and periodically reviewing consumption. Provide contracting flexibility by employing optional CLINs within appropriate resource categories to accommodate future growth.

As always, the FISMA security categorization will be essential in determining the available pool of CSPs that can be leveraged by contractors. Integration considerations for related applications impact hosting CSP selection for performance and manageability reasons based on where those resources are hosted and the nature of the system interactions. Again, effective comprehensive documentation of your existing IT system state is the key to contractor success in their proposed solutions.

Contract Vehicle Options

For a sizable component agency within a large agency, with multiple department level enterprise management consolidation efforts in various stages of implementation at play, a standalone single contract for a project of this scope may not be a common procurement.

This play is composed of major steps involving at least three main phases. Potentially the biggest phase in both cost and schedule risk is the application preparation phase. The overall scope of this effort will favor either specialty cloud migration focused contract vehicles (e.g., ACCENT) or IT solutions-based general purpose GWAC vehicles (e.g., Alliant, CIO-SP3). They will provide the flexibility in scope to handle the potentially significant resource effort needed to reengineer the application. GSA's Schedule 70 is a potential option as well with the solicitation spanning both SIN 132-40 for the cloud services and SIN 132-51 for the professional services needed to execute both the application refactoring and the hosting transition efforts. Delivery-order based GWACs (e.g., SEWP and CIO-CS) have fewer germane services and are less applicable as the application development effort for refactoring, combined with the transition support services result in the required professional services dominating the project.

DHS has established separate contracting solutions for commercial commodity-based IaaS cloud hosting services (DHS Enterprise Computing Services [ECS] BPAs) versus the professional IT services needed for supporting those CSPs. This model of having separate acquisitions can still effectively meet mission needs, albeit with a different set of tradeoff considerations based on the parameters. Consideration through governance processes and/or requirements within the professional services solicitation will need to be made to manage system integrator consumption of hosting resources they are not providing. Contractors should be required to provide estimates of cloud hosting resources anticipated to be used and be held accountable to those estimates.

Scenario 3: Refining Cloud

	Services Sought			
	Inventory / Assessment	Application Preparation	Migration Support	CSP
3 - Refining	Have	Have	Need	Need

Figure 22. Visual Scenario Reference, Refining Cloud

Initial Conditions

- A significant portion of the agency infrastructure is already in the cloud.
- You will migrate all remaining on-premise cloud capable mission and mission-support applications to another cloud provider.
- Enterprise architecture and IT governance processes are functioning well, and application system documentation is both sound and current.
- You are in a medium sized – large agency (110,000 employees).
- You are the most experienced deputy CIO with a mission area facing role.
- The agency has a national presence across the United States.

Additional Assumptions

- IT system inventory is current, comprehensive, and reliable.
- Single acquisition and existing support contracts will not be leveraged beyond current levels.

Checklist

- ❑ Data rights and movement conditions are documented as a requirement.
- ❑ Documented support plan during migration.
- ❑ Post-migration application support strategy.
- ❑ Post migration support and communications plan for mission area application users.
- ❑ Network architecture and connectivity – TIC compliance is met and required common services for integrations are available within required service levels.
- ❑ Cost planning strategies.
- ❑ 1.4.3.4 Key Questions
- ❑ Is your security breach and notification plan thorough, compliant, and resilient?
- ❑ What are the changes you plan to make to disaster recovery and COOP plans?
- ❑ Will your service level definitions accommodate this delivery plan? How will you maintain surveillance and balance competing requirements?
- ❑ Are targeted applications cloud-ready?
- ❑ Do you have a requirements definition that clearly defines duties of the provider relative to duties of the government?
- ❑ Do you have a full understanding of affected software licensing that will move to the cloud?
- ❑ Are your administration rights, delegation, and credential issuing plans sound?
- ❑ Do you have the governance in place to manage provisioning (ordering) and de-provisioning of cloud services?
- ❑ Do you have a requirements definition that clearly defines duties of the provider relative to duties of the

government?

- ❑ Do you have a comprehensive set of service level agreement requirements? Does it include acceptable application performance metrics?

Discussion

Migration Support

The essence of this project scenario is getting applications out of the legacy on-premise data center and to the cloud. As the application inventory is complete, the scope of cloud-ready applications included in this migration effort should be well defined as are the major integration and dependency hurdles, all of which can be provided in the solicitation to describe the as-is state of the agency enterprise. A separate CSP is specified for hosting these applications to provide enterprise resiliency and flexibility. The new environment will need configuration planning and architectural standards development and specification. This may be straightforward due to the “green field” nature of a new CSP but may require additional effort to ensure common services across the enterprise such as identity, credential, and access management (ICAM) and enterprise resource monitoring are available and uniformly instantiated. Likely an agency of this size will have some IT assets already hosted in the target CSP but they are expected to be isolated and inconsequential relative to the scope of this project scenario. Further, the national presence of the agency may warrant deployment on multiple regions within the CSP for performance purposes depending on the nature of the applications.

To achieve success, leverage repeatable processes that are well integrated to the agency configuration management and governance processes. The overall scheduling of the transition of individual applications can be a complex challenge based on the interdependencies between applications. These challenges may be further complicated by the extended multi-CSP architecture in place. As the number of applications grows, expanding the project scope and likely manifesting interdependency driven scheduling challenges, the contract structure may necessitate phased implementation approaches with multiple milestones breaking the project into lower risk chunks. As always, the goal is to balance between execution flexibility and effectively holding contractors accountable for meaningful performance in support of mission.

Even though the targeted applications are cloud ready, consider security requirements for each application as part of the migration. This can include, and may necessitate, internal application component security analysis. Migration activities should consider data preparation, in addition to the interface and service transition planning steps. Cutover planning combined with go-live support are key considerations along with an appropriate back out or rollback plan for when (not if) things go wrong.

Consideration of a cloud management platform implementation, capable of supporting the multiple clouds deployed across the enterprise, is appropriate if one is already in place. However, implementation of a successful cloud management platform may be better served as a separate project to enhance opportunities for solution flexibility rather than tacking it onto this acquisition.

Include comprehensive and relevant specifications for the as-is environment and agency architectural models and goals for the to-be environment to support successful and competitive contractor proposal responses. Depending on the number of applications targeted for migration, consider separate CLINs for each application or groups of applications. This provides flexibility in execution and funding for the government. Further, for a large number of

applications, a separate CLIN could be designed specifically for scheduling and project management functions.

CSP

This scenario represents a novel case where a particular CSP[35] is used for hosting, and a specific provider is purposely not leveraged to specifically provide for vendor diversity to enhance resiliency. The agency's national presence may increase the likelihood that some application or application interaction characteristics exist that necessitate a CSP with particular attributes such as multiple regions for potentially more localized resource deployment.

Provide a robust description of hosting needs to ensure the workloads will function effectively and that the CSP supports any known specialized performance characteristics. Standardized resource consumption estimates provide both an overall scope of effort to contractors and a potential path to price evaluation within this component when needed. Appropriate CSP resource consumption metrics will vary by situation, but can include overall numbers of, for example, VMs with levels of RAM and vCPU cores, total required block storage, among other resources.

Anticipate and plan for future expansion of required CSP capacity but do not commit to requirements beyond current needs. The goal is to build in flexibility for anticipated and potential increases and decreases in cloud service consumption based on reasonable assumptions. Optional CLINs can be valuable tools to achieve this flexibility.

Contract Vehicle Options

There are many contracting vehicle options to meet the basic requirements of providing significant hosting capacity combined with considerable IT support labor to implement the transition. The biggest project specific factor that influences the available choices will be the number of systems moving and their interdependencies. These factors increase the overall amount of IT services support involved in the overall acquisition. Additionally, as this complexity increases, actual system transition execution phases may be introduced thereby lengthening overall implementation timelines and necessitating more sophisticated contract structures. These higher complexity enterprise level projects will favor the general-purpose IT solutions-based contracts (e.g. Alliant, CIO-SP3) over the delivery-order based GWACs (e.g., CIO-CS, SEWP). Cloud-focused contracts including transition support services such as DOI's FCHS or an available agency-specific option can be considered in addition to the utility belt of IT contracting, Schedule 70.

Scenario 4: Tuning Cloud

	Services Sought			
	Inventory / Assessment	*Application Preparation*	*Migration Support*	*CSP*
4 - Tuning	Have	Have	Have	Need

[35] CSP justification is discussed within other Scenarios.

Figure 23. Visual Scenario Reference, Tuning Cloud

Initial Conditions

- You have a rationalized and working cloud strategy that includes all cloud types.
- Recent experience indicates a sensitive mission area requires very high service levels and support responsiveness (relative to the remainder of the enterprise).
- The agency has an active, responsive, and accurate enterprise architecture function.
- You are in a large agency (175,000 employees).
- There is a single primary CSP and your contract ends in 21 months.

Additional Assumptions

- The performance of the current CSP is marginally acceptable.
- IT professional services support across the IT portfolio is in place and functioning well.

Checklist

- ❑ Documented lessons learned in the existing arrangement.
- ❑ Cost planning strategies.
- ❑ Data rights and movement conditions are documented as a requirement.
- ❑ Commercial cloud service deployment operations and process guide.
- ❑ Thorough market research for CSPs and their reseller channels.

Key Questions

- What are the changes you plan to make to disaster recovery and COOP plans?
- What service levels do you need that are different from those in use?
- What requirements or contract weaknesses exist in the current arrangement that limit achieving service that would go beyond basic expectations?
- Do you have the governance in place to manage provisioning and de-provisioning of cloud services?
- Are your financial and deployment management processes working well and ready to transition to support a new enterprise contract?

Discussion

CSP

This acquisition focuses on obtaining the cloud computing services directly. A key question and concern at this point will be whether there are requirements for a specific CSP based on the existing system landscape. Specifying a particular CSP will typically require justification as part of the solicitation. The type of justification may vary based on whether the CSP has multiple resellers (brand name or limited source) or if the CSP is directly contracting with the Government (sole source). Conversely, in a case where cross provider resiliency is required beyond regional workload distribution within the same CSP, it may be necessary to specify your current providers to exclude them from the proposal.

In the situation where the hosting requirements allow for more generic resources, competition can be enhanced since a range of CSP solutions can be brought forward. Describe the hosting needs sufficiently to be able to ensure the

workloads will function effectively and allow for an effective comparison between bids. Appropriate metrics vary by workload, but they can be very helpful to describe the range by percentage of, for example, VM's by RAM or vCPU cores, and/or IOPS and throughput of storage or networking performance. This can be important in obtaining effective cost estimates when diverse workloads are aggregated from across many components and combined into a single solicitation such as in this scenario. The particular capacity metrics utilized can vary significantly across service models. Software as a Service (SaaS) solution metrics can often be based on capabilities more closely aligned to the various application capabilities delivered and may not include as many technical measurements.

Anticipate and plan for future expansion of required CSP capacity, but do not commit to requirements beyond current needs. The goal is to build in flexibility for anticipated and potential increases and decreases in CSP service consumption based on reasonable assumptions. Optional CLINs are valuable tools to achieve this flexibility.

Require CSP solutions compliant with *The NIST Definition of Cloud Computing* to avoid solutions that are only called "cloud" and to ensure your agency fully leverages its benefits. FISMA security categorization for the hosted systems is a key constraint on the ability of the provider to meet security requirements. There are far fewer FedRAMP High provisional authorizations than FedRAMP Moderate. This constraint has more impact within DoD with their four separate Impact Levels as defined in the Cloud Computing Security Requirements Guide (SRG). Consider whether to require FedRAMP authorization at the time of solicitation. It will save time on deployment by lowering the risk of achieving security authorization in a timely manner but may create challenges if the pool of capable providers is too small.

Billing management requirements are often overlooked for a typical CSP-only acquisition. As hundreds or thousands of individual resources can easily be deployed across the enterprise, managing the consumption is a significant challenge. Ensure that methods exist to help mark resources by organizational unit, by application within that organizational unit, and by environment (e.g., dev, QA, prod). Require CSPs provide API driven access to billing data and resource consumption details. Building on this, ensure CSP integration capability with agency systems and prepare agency processes to support effective management of resource consumption.

Contract Vehicle Options

With the scope of the acquisition narrowed down to a single well-defined category, potential contract vehicle identification is simplified. There are numerous government-wide options available, but few have pre-evaluated cloud solution compliance with the NIST cloud computing characteristics. General-purpose players include the delivery-order based GWACs (e.g., SEWP, CIO-CS) and Schedule 70 which features the Cloud SIN 132-40 with pre-vetted NIST compliant offerings. DOI's Foundation Cloud Hosting Services (FCHS) also is a viable option as it is open to government-wide use and has vetted solutions for the NIST cloud characteristics. The major IT solutions contracts (Alliant, CIO-SP3) are not suitable options when only procuring commodity cloud services. Some agencies have other specific options such as the Army ACCENT blanket ordering agreement (BOA) and the DHS ECS BPA. Having removed the requirement for professional services, lowest price technically acceptable (LPTA) evaluation becomes an option.

Contract vehicle access to CSPs differs based on the service model, especially for SaaS. Comprehensive IaaS providers that deliver a range of typical hosting services including various sized VM's, storage options, and flexible

programmatic networking capabilities, are typically well represented on vehicles. SaaS providers may not be generally available on multiple government-wide contracts due to licensing exclusivity with their channel partners.

Appendix D: Glossary of Terms

1. **Account**. Provisioned identity able to manage infrastructure and platform services.
2. **Addressing**. Data used to route data (e.g., IPv4, 1Pv6).
3. **Administrative Access**. Access to DoD above that of a normal user, such as privileged access to services, keys, management, or auditing tools.
4. **Allocation**. Server resources dedicated to DoD customer as measured by CPU and GPU capacity.
5. **Antifragile**. Robustness increases in response to volatility, attacks, and failures.
6. **Application**. A single computer system deployable to a single virtual machine. This may include connections to other applications, databases, network interfaces, etc.
7. **Application Refactoring**. The product of modifying an existing code base to significantly improve the performance and technical architecture of the code; and is not primarily motivated to change the code functionality. Typically, this is an aggregate set of refinements, enhancements, and modifications that are potentially not justified by resource input to perform alone but are expected to have a major improvement when performed holistically. Changes, modifications, and enhancements can include elements such as database changes and code reorganization.
8. **Classified Infrastructure**. Classified infrastructure compliant with DoD Impact Level. 6 as defined in the DoD CC SRG and coupled with the controls in the CNSSJ 1253F Attachment 5: Classified Information Overlay lD 221.
9. **Classified Media**. Infrastructure impact level 6 and above.
10. **Cloud Enabled**. A software application or workload that is both ready to be hosted in an IaaS (or PaaS) cloud environment and has some capability to leverage the cloud characteristic of rapid elasticity. The expectation is of only a minimal amount of configuration effort would be required to deploy (or re-deploy) the application in the cloud.
11. **Cloud Service Models**. The below cloud service models are three of the most common service model offerings. The service models can be offered in General Purpose, Fit-for-Purpose, and Internal clouds. Additionally, these service models can be provided by commercial vendors or owned and operated by the Department.
    - **Infrastructure as a Service (IaaS).** The capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).
    - **Platform as a Service (PaaS).** The capability provided through software, on top of an IaaS solution, that allows the consumer to replicate, scale, host, and secure consumer-created or acquired applications on the cloud infrastructure. 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.
    - **Software as a Service (SaaS).** The capability provided to the consumer is 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.
12. **Cloud Service Provider**. A service provider that owns, maintains and enhances their services, and houses those service elements in a location that they own. Service is usually delivered via the internet or other

network connection. Customers usually pay on a routine cycle and at a rate usually based on their usage that period or at a recurring standard rate.

13. **Cloud**. The practice of pooling physical servers and using them to provide services that can be rapidly provisioned with minimal effort and time, often over the Internet. The term is applied to a variety of different technologies (often without clarifying modifiers), but, for the purpose of this document, cloud refers to physical computing and storage resources pooled to provide virtual computing, storage, or higher-level services.
14. **Commercial Cloud**. Computing, storage, and network resources and services that a commercial provider maintains, operates, and manages and that are made available to multiple customers (as opposed to cloud resources and services owned and operated by an organization for their own benefit, for example). Depending on the contract, the commercial cloud service provider may be performing in commercial facilities or on-premises in Government facilities. As examples, JEDI Cloud will be performed in commercial facilities whereas milCloud 2.0 is on-premises in Government facilities.
15. **Cryptographic Certainty**. Assurance [δ.7] unmediated data transfer does not occur.
16. **Data Center**. A physical site containing significant infrastructure.
17. **Drawdown Accounts**. An organizational method for paying for a cloud service. The consuming organization pays the provider a set amount of money. The provider decrements the money put into the account relative to what the consuming agency is using.
18. **Failover**. Unanticipated migration of application operation with minimal downtime.
19. **Fit-for-Purpose (F2P) Cloud**. A cloud environment that meets highly specialized mission requirements that cannot easily be met through a General Purpose Cloud solution and is suitable for scaling to adopt new DoD customers at the enterprise level. Determination criteria include utility for mission, ease of management (including provisioning and reporting), and contract terms.
20. **General Purpose Cloud**. Infrastructure and Platform as a Service offerings that meet the majority of the DoD's cloud computing needs across all Components of the enterprise organization.
21. **IaaS**. Infrastructure as a Service. A service model describing an offering from a provider that allows a customer to purchase compute, storage and network services on demand. IaaS is priced by a consumption unit. The customer pays for the service used during the period based on a per consumption unit price.
22. **Impact level**. Sensitivity and security requirements [δ.6] for data.
23. **Infrastructure**. Physical and virtual components that comprise JEDI.
24. **Internal Cloud**. Specific F2P solutions for systems and applications that need to operate in a private, on-premises cloud environment due to security or operational reasons.
25. **Investigation**. Response to potential or actual attack, intrusion, or compromise of the DoD assets/data residing on the CSP.
26. **Logical Separation**. Non-physical means to provide isolation between tenants, with controls in place to assure prevention of unmediated data transfer.
27. **Migration**. The act of moving an application from one infrastructure or platform to another infrastructure or platform. Typically, this will require intermediate work to refactor the code to suit the new platform.
28. **Modernization**. The act of taking existing software or hardware and rebuilding it using modern methodologies and technologies. As an example, an outdated COBOL-based financial billing system might be modernized and developed as a modular, containerized micro-service backend architecture and single page application front end. Alternatively, this could mean taking a physical server that is limited in processor speed, memory, and storage space and replacing it with a more modern machine that makes use of modern processor architectures and networking protocols.
29. **Network**. Physical infrastructure related to packaging or transmitting data (e.g., router).
30. **PaaS**. Platform as a Service. A service model describing an offering from a provider that allows a customer to make on demand purchases. The types of services included in this model are broad and loosely defined as those infrastructure and end user applications. PaaS is priced by a consumption unit. The customer pays for the service used during the period based on a per consumption unit price.
31. **Rationalization**. The process of determining if an application should be refactored and migrated to a new

platform, left on its legacy platform as-is, or sunset.

32. **SaaS**. Software as a Service. A service model describing an offering from a provider that allows a customer to purchase the use of the software on demand. The software has a single code base and is available to many different organizations and individuals that may or may not be affiliated. SaaS is priced by a consumption unit. The customer pays for the amount of service used during the period as a function of the price consumption unit or by a standard subscription fee.
33. **Server**. Physical infrastructure related to transforming or storing data (e.g., database).
34. **Subscription-Based**. A payment arrangement between a provider and customers. Consumers and consuming agencies pay a fee to access the service the user provides. This payment type is not based on how much the consumer uses, but whether or not the user has on-demand access to use the service
35. **Tactical Edge**. Means environments covering the full range of military operations, including, but not limited to, forces deployed in support of a Geographic Combatant Commander or applicable training exercises, on various platforms (e.g., dismounted infantry patrol, forward operating base, and aircraft carrier) and with the ability to operate in austere and connectivity-deprived environments.
36. **Testing**. Assessments and attacks to verify and validate security compliance, survivability, operational resilience and incident response through shared responsibilities for the CSO, supporting infrastructure, and the interfacing infrastructure for networks physically or logically connecting to the end user.
37. **Traffic**. Internal or external, ingress or egress as measured in bytes.
38. **Unclassified Media**. Infrastructure handling impact level 5 and lower.
39. **US Soil**. All possessions and territory over which sovereignty of United States extends.
40. **Vulnerability**. Weaknesses affecting data transfer, service availability, code execution, or enabling unauthorized actions.

Appendix E: Acronyms

Table 22 provides a list of acronyms used in this document.

Table 22. List of Acronyms

Acronym	Definition
3PAO	Third Party Assessor Organization
AO	Authorizing Official
AoA	Analysis of Alternatives
API	Application Programming Interface
AT&L	Acquisition, Technology, and Logistics
ATO	Authorization to Operate
C&A	Certification & Accreditation
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CDD	Capability Development Document
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CL	Confidentiality Level
COMSEC	Communications Security
CONOPS	Concept of Operations
COTS	Commercial off-the-Shelf
CPD	Capability Production Document
CPI	Critical Program Information
DAA	Designated Accrediting Authority (older term replaced with Authoring Official)

Table 22. List of Acronyms

Acronym	Definition
DAG	Defense Acquisition Guidebook
DASD	Deputy Assistant Secretary of Defense
DAU	Defense Acquisition University
DBS	Defense Business System
DIACAP	DoD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DITPR	DoD IT Portfolio Repository
DoD	Department of Defense
DODI	DoD Instruction
DoDIN	DoD Information Networks
DOT&E	Director of Operational Test & Evaluation
DT&E	Developmental Test and Evaluation
EMD	Engineering & Manufacturing Development
FedRAMP	Federal Risk and Authorization Management Program
FIPS PUB	Federal Information Processing Standard Publication
FISMA	Federal Information Security Management Act
FRP	Full Rate Production
FRP/FD	Full Rate Production/Full Deployment
GOTS	Government off-the-Shelf
GSS	General Support System
IA	Information Assurance

Table 22. List of Acronyms

Acronym	Definition
IA	Independent Assessor (3PAO)
IaaS	Infrastructure as a Service (Model)
IAS	Information Assurance Strategy (older term, now called Cybersecurity Strategy)
IATO	Interim Authorization to Operate
IC	Intelligence Community
ICD	Initial Capabilities Document
ID	Identification
IIL	Information Impact Level
IMP	Integrated Master Plan
IMS	Integrated Master Schedule
IOT&E	Initial Operational Test and Evaluation
IPT	Integrated Product Team
IS	Information System
ISSO	Information System Security Officer
IT	Information Technology
JCIDS	Joint Capabilities Integration and Development System
KPP	Key Performance Parameter
LAN	Local Area Network
LCSP	Life-Cycle Sustainment Plan
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MDD	Materiel Development Decision

Table 22. List of Acronyms

Acronym	Definition
MS	Milestone
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVD	National Vulnerability Database
O&S	Operations and Support
OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
OT&E	Operational Test and Evaluation
OTA	Operational Test Agency
P&D	Production and Deployment
IaaS	Infrastructure as a Service (Model)
PCA	Physical Configuration Audit
PDR	Preliminary Design Review
PEO	Program Executive Office
PIA	Privacy Impact Assessment
PIT	Platform Information Technology
PM	Program Manager
PMO	Program Management Office
POA&M	Plan of Action and Milestones
POC	Point of Contact
PPP	Program Protection Plan
RA	Risk Assessment

Table 22. List of Acronyms

Acronym	Definition
Rev.	Revision
RFP	Request for Proposal
RMF	Risk Management Framework
SA	Security Assessment
SaaS	Software as a Service (Model)
SAR	Security Assessment Report
SCA	Security Control Assessor (RMF terminology)
SCRM	Supply Chain Risk Management
SDD	System Design Document
SDLC	System Development Life Cycle
SDS	System Design Specification
SE	Systems Engineering
SEP	Systems Engineering Plan
SME	Subject Matter Expert
SP	Special Publication
SRR	System Requirements Review
SSE	Systems Security Engineering
SSP	System Security Plan
STIG	Security Technical Implementation Guide
T&E	Test and Evaluation
TA	Threat Assessment
TMRR	Technology Maturation and Risk Reduction

Table 22. List of Acronyms

Acronym	Definition
TSN	Trusted Systems and Networks
USD	Under Secretary of Defense
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
VA	Vulnerability Assessment
WIPT	Working-Level Integrated Product Team

Appendix F: References

Table 23 provides a list of references cited in this document.

Table 23. List of References

References
25 Point Implementation Plan to Reform Federal Information Technology Management: December 2010, U.S. Chief Information Officer (U.S. CIO) Vivek Kundra directed Federal agencies towards a “Cloud First” policy.
44 U.S. Code Chapter 21, National Archives and Records Administration
44 U.S. Code Chapter 31, Records Management by Federal Agencies
Amazon Web Services – SEC (OCIE) Workbook, Dated May 2015
Army, Army Cloud Computing Strategy, March 2015
Application Rationalization Playbook – Cloud Smart and the CIO Council 2019 https://www.cio.gov/assets/files/Application-Rationalization-Playbook.pdf
Carnegie Mellon, CERT Resilience Management Model--External Dependencies Management (EXD), February 2016
CIO Council, Creating Effective Cloud Computing Contracts for the Federal Government, February 2012
CIO Council, Federal Shared Services Implementation Guide, April 16, 2013
Clinger-Cohen Act (CCA)7: Requires every Federal government organization to have a CIO, who is responsible for maintaining information security and privacy.
Cloud Security Alliance (CSA) FedRAMP Cloud Controls Matrix-v3-0-1 Candidate Mapping
CNSS Instruction 1253F Attachment 5: Classified Information Overlay, dated May 9, 2014

Table 23. List of References

References
CNSS Instruction l253F Attachment 3: Cross Domain Solution Overlay, dated September 12,2017
CNSS Policy 11: Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products, dated June 1, 2013
CNSS Policy 30: Cryptographic Key Protection, dated December 28, 2017
CNSSI 1253, Security Categorization and Control Selection for National Security Systems, March 27, 2014
CNSSP 25: National Policy for Public Key Infrastructure in National Security Systems, dated December 11, 2017
Committee on National Security Systems (CNSS) Policy 15: Use of Public Standards for Secure Information Sharing dated October 20, 2016
DFARS 252.239-7010: Cloud Computing Services
Department of Defense (DoD) Cloud Strategy, December 2018
DHS Cyber Resilience Review
DISA, Best Practices Guide for Department of Defense Cloud Mission Owners, August 2015
DISA, Cloud Connection Process Guide, Version 2, March 2017

Table 23. List of References

References
DoD Updated References for DevSecOps: "Reference Design Version 1.0 12 August 2019 (public)" https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf?ver=2019-09-26-115824-583 DoD A&S and CIO signed memo "Software Development, Security, and Operations for Software Agility" October 2019
DoD CIO Memo, Department of Defense Cybersecurity Activities Performed for Cloud Service Offerings, November 15, 2017
DoD CIO Memo, Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services, December 2014, http://www.esi.mil/contentview.aspx?id=585
DoD CIO Memo, Use of Enterprise Information Technology Standard Business Case Analysis, October 23, 2014: http://www.esi.mil/contentview.aspx?id=586.
DoD Digital Modernization Strategy (DoD Information Resource Management (IRM) Strategic Plan) July 12, 2019
DoD Directive 5220.22-M: National Industrial Security Program Operating Manual, dated February 28, 2006
DoD Directive 8100.02: Use of Commercial Wireless Devices, Services and Technologies in the Department of Defense Global Information Grid, dated April 23, 2007
DoD Directive Form 254: JEDI ID/IQ Contract Security Classification Specification
DoD Instruction 8520.03: Identity Authentication for Information Systems, dated July 27, 2017 and subsequent guidance dated June 2018
DoD Instruction 8530.01: Cybersecurity Activities Support to DoD Information Network Operations, dated July 25, 2017
DoD Instruction 8540.01: Cross Domain (CD) Policy, dated August 28, 2017

Table 23. List of References

References
DoD Memorandum: Cybersecurity Activities Performed for Cloud Service Offerings, dated November 15, 2017
DoD, Department of Defense Cloud Computing Security Requirements Guide (SRG) v1r3, March 6, 2017
DoD, Department of Defense Cloud Computing Strategy, July 5, 2012
DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), July 28, 2017
DoDM 5200.01, DoD Information Security Program: Overview, Classification, and Declassification, February 24, 2012
Electronic Communications Privacy Act of 19863: Protects consumers against interception of their electronic communication (with numerous exceptions).
Executive Order 12829 - National Industrial Security Program, dated January 8, 1993
DOD Cybersecurity T&E Guidebook v2, Change 1 April 2018; Addendum: Cybersecurity T&E of DoD Systems Hosted on Commercial Cloud Service Offerings (https://www.dau.edu/cop/test/Pages/Documents.aspx)
Fair Credit Reporting Act: Includes privacy rules for credit reporting and consumer reports.
Federal Acquisition Regulation (FAR) 2.101: Definitions
Federal Cloud Computing Strategy: February 2011, U.S. Chief Information Officer (U.S. CIO) Vivek Kundra identified benefits of cloud computing, an overall adoption process, and criteria for prioritizing systems migration to cloud.
Federal Cloud Computing Strategy (2018) From Cloud First to Cloud Smart (https://cloud.cio.gov/strategy/)

Table 23. List of References

References
Federal Information Security Modernization Act of 201411: authorizes DHS to assist the administration of agency security practices, coordinating across the federal government, and providing assistance to agencies. DHS is also tasked with overseeing “binding operational directives,” or “compulsory direction” to an agency “for the purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability or risk.”
Federal Trade Commission Act: Prohibits unfair or deceptive practices -this requirement has been applied to company privacy policies in several prominent cases.
Financial Statement Audit Requirements for Service Organizations (DoD Cloud Way Forward), DCIO Update March 7, 2019
FIPS PUB 140-2: Security Requirements for Cryptographic Modules, dated December 3, 2002
GAO, GAO-16-325, CLOUD COMPUTING: Agencies Need to Incorporate Key Practices to Ensure Effective Performance, April 7, 2016
GAO-16-325 Report, titled “Cloud Computing”, Dated: April 2016
Gramm-Leach-Bliley Act (GLBA): Governs the collection, disclosure, and protection of consumers’ nonpublic personal information for financial institutions.
GSA/OMB, Cloud Migration Services SOO Templates, December 2012
HIPAA Assessment Tool, HIPAA On-Site Survey, Dated April 1, 2014
https://www.fedramp.gov/
Information Technology Infrastructure Library (ITIL)-- ITIL is organized into a series of five volumes (the books): Service Strategy, Service Design, Service Transition, Service Operation and Continual Service Improvement (Reference: http://www.itil.org.uk/)
ISO/IEC 19086-1:2016, Cloud Computing and Distributed Platforms

Table 23. List of References

References
ISO/IEC 20000-1:2011, Information Technology -- Service Management -- Part 1: Service Management System Requirements
ISO/IEC 27001:2013: Information technology -- Security techniques -- Information security management systems -- Requirements
ISO/IEC 27002:2013: Information technology -- Security techniques -- Code of practice for information security controls
ISO/IEC 27003:2010: Information technology -- Security techniques -- Information security management system implementation guidance
ISO/IEC 27004:2009: Information technology -- Security techniques -- Information security management -- Measurement
Joint Publication (JP) 3-12 (R): Cyberspace Operations, dated February 5, 2013
National Security Telecommunications and Information Systems Security Advisory Memoranda (NSTISSAM) Level I: Compromising Emanations Laboratory Test Standard
Navy Cloud Brokerage Policy, dated December 19, 2017
National Defense Authorization Act (NDAA) for Fiscal Year 2012, Section 2867 Data servers and centers, dated December 31, 2011
NIST Cybersecurity Framework (CSF)
NIST RMF, https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview
NIST SP 800-63: Digital Identity Guidelines, Revision 3 dated June 2017
NIST SP 800-88: Guidelines for Media Sanitization, Revision l dated February 5, 2015

Table 23. List of References

References
NIST Special Publication 500-299, NIST Cloud Computing Security Reference Architecture -- Draft
NIST Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing, Dated: December 2011
NIST Special Publication 800-146, Cloud Computing Synopsis and Recommendations, Dated: May 2012
NIST Special Publication 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations
Draft NIST Special Publication 800-171B Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations Enhanced Security Requirements for Critical Programs and High Value Assets, June 2019
NIST, NISTIR 7956, Cryptographic Key Management Issues and Challenges in Cloud Services, September 2013
NIST, SP 500-299, NIST Cloud Computing Security Reference Architecture (Draft)
NIST, SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010
NIST, SP 800-125, Guide to Security for Full Virtualization Technologies, January 2011
NIST, SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing, December 2011
NIST, SP 800-145, The NIST Definition of Cloud Computing, September 2011 (errata as of 161 April 27, 2012)
NIST, SP 800-292, NIST Cloud Computing Reference Architecture, September 2011
NIST, SP 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010 (Updated 6/5/2014)

Table 23. List of References

References
NIST, SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (includes updates as of 01-22-2015)
NIST, SP 800-53A Revision 4, Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans, December 2014
NIST, SP 800-60, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008
NISTIR 8006: Cloud Computing Forensic Science Challenges, dated June 30, 2014
Office of Management and Budget (OMB) Memorandum M-08-058 (also known as Trusted Internet Connection (TIC) initiative): meant to standardize and optimize security of internet connections used by the Federal government. The initiative is intended to improve security posture, monitoring and incident response by reduction and consolidation of external network connections.
Office of Management and Budget (OMB), Security Authorization of Information Systems in Cloud Computing Environments (Washington, D.C.: Dec. 8, 2011).
OMB Circular No. A-130: Managing Information as a Strategic Resource, dated July 28, 2016
OMB, 25 Point Implementation Plan to Reform Federal Information Technology Management, December 9, 2010
OMB, Federal Cloud Computing Strategy, February 8, 2011
OMB, Federal Information Technology Shared Services Strategy, May 2, 2012
OMB, Guidance on Exhibit 53—Information Technology and E-Government, July 1, 2013
OMB, Memorandum for Chief Information Officers, Security Authorization of Information Systems in Cloud Computing Environments, December 8, 2011

Table 23. List of References

References
OMB, Memorandum for Federal Chief Information Officers, Increasing Shared Approaches to Information Technology Services, May 2, 2012
OMB, Memorandum for Heads of Executive Departments and Agencies, Preparing for and Responding to a Breach of Personally Identifiable Information, January 3, 2017
TIC Reference Architecture 2.09: introduces new capabilities and clarifies existing mandatory critical capabilities, including recommended capabilities based on evolving technologies and threats.

Appendix G: NGA's Annex D, Cloud Data Guidance

ANNEX G: CLOUD DATA GUIDANCE

Version 5.1

12 January 2017

TABLE OF CONTENTS

TBD/TBR

UNCLASSIFIED		
TBD/TBR Log		
TBD	***TBR***	***Description***
002		NGA Metadata Catalog
003		NGA Service Registry, assumed to be a COTS product, under selection.
004		Guidance for Corporate Data
005		NGA Enterprise Log Repository

REVISION SUMMARY

UNCLASSIFIED		
Version	***Revision Date***	***Revision Summary***
1	12/31/2015	Initial Release
2.0	02/29/2016	Cloud Data Guidance V2: Updated Storage Guidance. Added Migration and Metadata Guidance.
3.0	4/19/2016	Cloud Data Guidance Coordination draft. Reorganized section, moved storage guide materials to white paper, revised most sections.
4.0	6/30/2016	Minor edits and corrections. More info on OpenDataStore. Moved cost section to another annex.
4.1	08/05/2016	Updated classification/portion marking to support push to SBU
5.0	9/30/2016	Added data movement process descriptions, and chart. Edited migration sections for consistency. Added data conditioning explanation. Revamped S3 Example Case. Added Database Example Case, and S3 Bucket Naming Standards.
5.1	1/6/2017	Added data Access section. Changed ‘Data Owner’ to ‘data custodian’. Revised migration sections for clarity and consistency. Extensive revision to Appendices D,E,F,G,H. Other Minor edits. New and substantively revised sections are so marked in the header and TOC, e.g. (*NEW*!).

1 INTRODUCTION

The goal of this document is to provide high-level Cloud Data Guidance, establish common terminology for cloud data service offerings, provide data migration guidance, and describe how NGA will manage its metadata. This annex describes aspects of cloud data architecture and migration, guided by the five goals of the NGA Unified Data Strategy, below.

Table 1: NGA Unified Data Strategy Goals

Goals	*Definitions*
Find the Data	Users across NGA, the IC and DoD are able to intuitively discover, access, and retrieve the geospatial data and content
Free the Data	Data are required to be separated from individual applications, systems and information silos
Protect the Data	Data accessibility is based on user role and access control data attributes, reflecting user rights, roles and data usage; available when and where needed
Automate the Data	Data are conditioned with metadata throughout its lifecycle to enable automated access, discovery, pedigree, provenance, retrieval, and analysis
Unify the Data	Integrated Intelligence is unified across all boundaries: architectures, security domains, geographic locations, and mission, corporate and functional operations

This document addresses key data requirements and offers recommended best practices to programs adopting cloud services. As the Agency migrates activities to cloud environments, data guidance will help define the data architecture, tools, and processes required to achieve success. Key overarching concepts of this guidance include that NGA data will be required to be:

- Managed in accordance with NGA data management, retention and records management policy
- Encrypted in transit and at rest
- Available to the NSG and IC community
- Cataloged and as applicable indexed for discovery (e.g. using the OMNI service and Search Engine services)
- Consistently tagged with handling and access information
- Exposed via services

The intended audience is program managers, software solution engineers, security engineers, security analysts, system administrators, and other stakeholders with responsibility for migrating new or legacy capability to a cloud environment.

The following Section 2 reviews cloud data concepts and offers general guidance. Section 3 describes the migration process step by step, and Section 4 addresses metadata considerations. Appendix I presents two paths for evolving to the cloud architecture, to assist Data Stewards and Program Managers design a customized appropriate path for their own data.

2 CLOUD DATA GUIDANCE

The Cloud Data Guidance provides Chief Data Officer (CDO) direction on how to handle Data and Metadata in the cloud. It contains information specific to migration, as well as information for the transition and steady state beyond migration.

2.1 Key Concepts

The concepts introduced and defined in this section will enable the reader to better understand the guidance issued later in this document, including OpenDataStore, Analytic Data Lake, Conditioning, Data Migration Categories, ContentID and Roles.

2.1.1 Multiple Environments – TC, SC and UC

The Cloud as referred to in this Guidance includes the

- Top Secret Cloud (TC)
- Secret Cloud (SC)
- Unclassified Cloud (UC).

These are distinct intranets serving the IC and DOD communities, and the classified ones are air-gapped. In general, the Guidance applies to all of these environments, with exceptions noted. The initial priority is migrating data to the TC.

2.1.2 Data Access (*NEW*!)

In alignment with DNI directives, the Data Access architecture for Mission Data has the following features:

- There is an automated way to discover and access data. All data is metadata tagged, personnel identities or roles are associated with accessibility attributes, and automated rules and processes will use these tags to automatically enforce accessibility and dissemination policy.

- *Responsibility to provide* is achieved. The default stance on Data is that it is shareable, unless there is a specific dissemination control, exemption or constraint preventing it from being shared. However, *responsibility to provide* does not negate our responsibility to protect sources and methods.

- People with the "*appropriate security clearance and an assigned mission need",* as indicated by their security attributes and groups they are assigned to, are able to

access data with corresponding attributes and groups. These entitlements are how *need to know* is expressed and implemented.

- No other 'need to know' check is performed – it is implicit in the request.

Section 5 outlines the concepts needed to achieve the future architecture and the final end state desired. The focus is on data access authorization rather than identity validation or other aspects of network or application access.

2.1.3 OpenDataStore: All Data for All Missions

The OpenDataStore represents an architectural evolution. In the past, data belonged to and was stored and managed by applications often in semi-private data structures. In the future, data will be managed by enterprise data services and maintained in common areas accessible to all authorized users, even if the user and use is unanticipated, illustrated in simplest terms in Figure 2-1. This concept is further described in the Design Whitepaper on Target Data Architecture.[36]

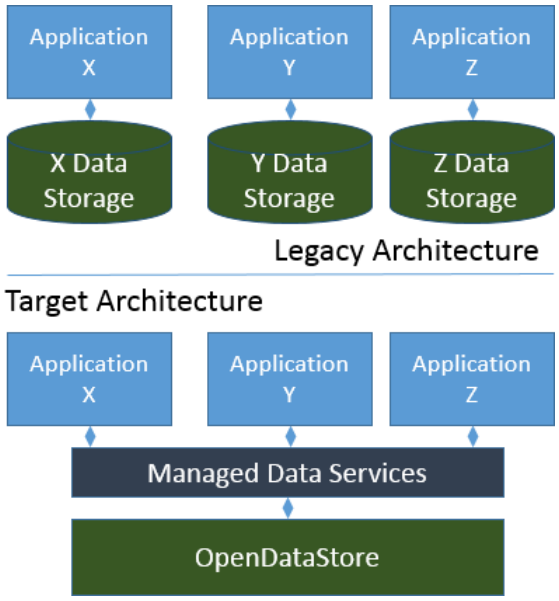


Figure 2-1: Legacy and Target Data Architecture

The OpenDataStore contains both persistent storage of data accessible to end users for normal work and analysis, and data services. It is a highly inclusive concept covering all data stored for normal end-user use. It encompasses all means and methods to store data, from flat files, to relational databases, NoSQL databases and complex structures like data warehouses and Analytical Data Lakes. It also includes all formats, from structured relational, to object, to triple-store, to unstructured files. It is an amalgamation of two concepts: Open Data and the Data Store. A Data Store is an inclusive repository, and the Open Data movement advocates

[36] Design White Paper - Cloud Target Data Architecture Considerations, CAMG, 2016.

that data should be freely available to everyone to use and republish as they wish.

Files can be stored in Amazon Web Services AWS)/C2S (Commercial Cloud Services) S3 buckets or in File System implementations on C2S EBS (Elastic Block Services- raw data storage area). Relational and NoSQL databases may be supported by C2S RDS (Relational Database Services) or with C2S Dynamo. Other services can be set up in an C2S EC2 (Elastic Compute Cloud- Amazon virtual machine service) instance with EBS. Data Transformation and Conditioning services are among the many types of Data Services that NGA can stand up. See Figure 2-2.

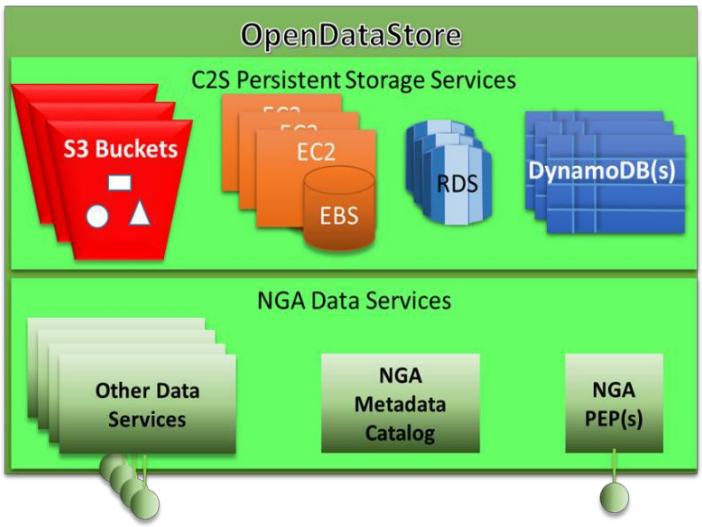


Figure 2- 2: OpenDataStore

While the Open Data movement is about making data free and open to the public, that cannot be done with classified and controlled information. What can be done includes:

- Automate the access via Policy Enforcement Points (PEPs) so if the user credentials meet the metadata attributes, the user can access the data. There would be no need to go through a specific owning application to get data. Anyone with the rights could get the data, which is now a community asset.
- Eliminate technical barriers (including excessive organization by application and use of private data formats) to mission data, beyond that required by the classified networks.
- Design data access services that meet user needs, including services that allow dataset wide discovery and access when appropriate.

OpenDataStore: Managed Data Services

The ultimate objective is to provide all data as a *Managed Service*. Initially, this will take the form of providing a shared environment to store data: the OpenDataStore. The OpenDataStore will work much like the NGA Enterprise File Storage and Enterprise Database Clusters of the legacy NGA Data Centers:

- The Data Infrastructure will be set up for the Application Service Provider (ASP) programs
    - Data Infrastructure access rights and networking will be set up
    - Actual instances for data storage (database or file storage) will be made available to the ASP
- The ASP will be able to configure that data storage instance
    - The ASP can define role based access controls internal to their storage solution
    - The ASP can configure their storage solution to support their activity needs

One of the goals of the CDO is to ensure that the mission and/or activity capabilities are not adversely affected by the Cloud Data Migration. As such, initially the CDO will work to make sure, to the extent possible, that activities will be able to access their data the same way they were able to access their data in the past, to include direct connections to data storage.

Over time, the CDO, working with the ASPs, will work to transition all data access to web service based access instead of application-direct access to the data stores. Eventually, the ASPs will be consumers of the Data Services instead of working directly with the data stores.

OpenDataStore: NGA Content C2S/AWS Accounts

The CDO is creating a Content C2S Account for Mission Data and a Corporate C2S Account of Corporate Data for each security fabric on C2S. All Mission Data will be stored in the Content Account and all Corporate Data will be stored in the Corporate Account, per CDO Guidance.

Note: While other data categories are not required to go in either of the CDO accounts in the OpenDataStore, there is nothing preventing them from being stored there, should the data custodian so choose. There are many instances where Activity Data shares space with Mission Data in a database, and it may be easier to store the entire database in the Content Account than to divide the database.

OpenDataStore: Service Providers

There are 3 service provider roles with respect to the OpenDataStore:

Table 2: Service Provider Roles and Responsibilities

UNCLASSIFIED	
Provider Type	Rights & Responsibilities
Infrastructure Service Provider (ISP)	• Creation of AWS Accounts • Configuration/Management of the IAM (AWS Identity Access Management) services in the AWS console in any given account • Configuration/Management of the Network services in the AWS console in any given account

Data Service Provider (DSP)	• Management of the OpenDataStore Data Storage and Data Services • Configuration/Management of all the AWS services in the NGA Content AWS accounts except those managed by the ISP
Application Service Provider (ASP)	• Create/Read/Update/Delete (CRUD) operations in the various Data Stores needed by their Activity • CRUD operations against the NGA Metadata Catalog • Configuration of database accounts for databases related to their activity • Configuration/creation of database structures and database code • The ASP will **not** have the right to access the AWS console, or to spin-up or spin-down instances. They will just be able to access and perform whatever actions granted to them against the specific instances they need to access.

OpenDataStore: Assessment & Authorization (A&A)

The OpenDataStore extends the concept of the shared responsibility under which C2S operates:

- The C2S contractor (Amazon) has the responsibility for securing the hardware and virtual machines.
- The ISP has the responsibility for setting up NGA C2S accounts and ensuring IAM and network security. The ASP has the responsibility for the A&A of their activity, and for the storage service they are operating and configuring within NGA Content accounts.

Security has stated that activity boundaries do not align with C2S account boundaries, and that the activity A&A includes all parts of the activity architecture, not just the parts within their own C2S account. Furthermore, since the ASP is configuring their actual instance in the NGA Content accounts, they are responsible for showing that the configuration they performed meets ICD 503 requirements.

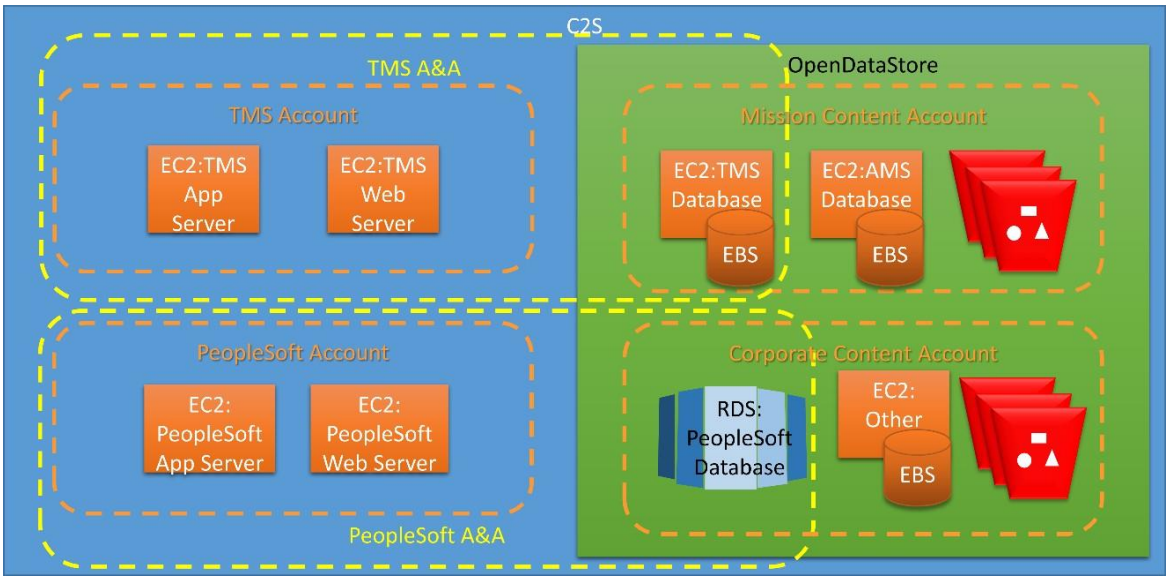


Figure 2-3: A&A Example

Figure 2-3 illustrates two examples. In the first example, the TMS (Target Management System) activity has a TMS Account where their Web and Application server instances reside. The TMS Database is on an EBS backed EC2 instance in the Mission Content Account, so the TMS Activity Architecture spans two C2S accounts, and the TMS Activity is responsible for the A&A for its entire Activity Architecture. The DSP would spin up the instance, using the established standard Oracle with Spatial AMI (Amazon Machine Image) and provide the secure access credentials to the Activity. The Activity would then set up individual developer staff logins within that instance and any other configurations required to be ICD 503 compliant in order to achieve Authority to Operate (ATO) for their activity, and that Oracle Database instance. However, since they are using the standard AMI, ATO is bounded by their ASP Activity.

In the second example the PeopleSoft application and web servers are in a PeopleSoft account, but the PeopleSoft database is on the RDS managed service in the Corporate Content Account. The DSP stood up the RDS instance for the ASP, but the ASP is responsible for setting up their schema, setting up developer accounts in Oracle along with other infrastructure tasks. The ASP is still responsible for the A&A of the entire PeopleSoft Activity Architecture, even though it spans the PeopleSoft Account and the Corporate Content Account.

In both cases, there will have to be test cases that prove that the ASP NIST 800-53 controls are satisfied. In summary, the ISP, the DSP and the ASP will each have NIST 800-53 controls that will need to be satisfied through test cases. The controls can be unique to a service provider or shared as negotiated with OCIO (CIO-T). However, A&A boundaries are not determined by hardware nor account boundaries. For additional information on the Cloud A&A process, see the Cloud Security Volume, Section 5.0.[37]

[37] Cloud Security Volume, Section 5.0, CAMG 2016.

OpenDataStore: Exceptions

The vision laid out for the OpenDataStore and the Roles and Responsibilities for the various service providers will support the needs of most Missions and Activities. However, it is understood that there may be exceptions based on security, policy or technical needs. For Activities that need more rights with respect to their data, or data that needs greater protections than are possible in a common C2S account, the CDO will work with the Activities and the Data Custodians on a case-by-case basis to determine what is needed to resolve their issues, and grant exceptions to the CDO Data Guidance if necessary.

2.1.4 Analytical Data Lake Concept

A Data Lake is a popular approach used worldwide for analysis of large amounts of data.

"A Data Lake is an attempt to bring together physically available data stores in such a way as they can be easily assessable to users." (Gartner[38]).

Characteristics common in commercial data lakes include:

- The data are typically sub-transactional (append only) or non-transactional (read only)
- Multiple user communities have questions of the data
- The data are of a scale/volume that they won't economically fit into a relational database (typically a repository built on inexpensive hardware for storing 'big data')
- Data may be "raw" (Data are in their native format and have not been transformed in some way in order to be ingested into the Data Lake)

The Data Lake is an Analytical tool. It allows the user to put massive amounts of disparate data in one spot and run analysis across all of it. It is not, however, a data repository for all data at NGA. For example, the production databases for Foundation GEOINT Data are updated tens of thousands of times per day, so these would not be able to exist in an "append only" or "read only" structure.

A Data Lake might not be permanent. It is possible that a Data Lake would be created to answer a specific question. The data sets needed would be loaded, the question asked and answered, and then the Data Lake taken down. So, rather than one, massive, permanent Data Lake at NGA, there could be many Data Lakes, created and taken down in response to Analytical needs.

A Data Lake risks becoming a Data Swamp or Landfill. If the data in the Data Lake is not properly conditioned/metadata tagged, then the data will not be discoverable. Tossing problem data into a Data Lake does not cure it of any problems.

The implementation of a Data Lake typically would be a Hadoop or Spark cluster, or, in the Intelligence Community (IC), often by an Accumulo cluster. Any could be readily set up in C2S.

---

[38] White, David, *The Confusion and Hype Relating to Data Lakes*, Gartner, June 2014.

2.1.5 Conditioning

Conditioning is formatting and metadata processing – cataloging and tagging -- of ingested data. Ingest conditioning is defined as that metadata and formatting work minimally required to allow successful load into persistent storage, including required Enterprise Data Header (EDH) handling information, and also allow for potential discovery. The scope is 'just enough' to achieve this without impeding load or causing unnecessary rejection of ingest data.

Conditioning may go farther and may be performed during ingest or at a later time.

- External metadata enhancements, including populating metadata catalogs, search engine indices, and semantic web links.
- Contextual metadata improvements, including database metadata, object wrappers and headers, and in-line tags such as XML microformats.

2.1.6 Data Migration Categories

Some Guidance varies depending on data migration category. These include:

- **Mission Data:** Data used in performance of the NGA Mission, which typically would be Gold Copy or Record data. This would include source data (host nation publications, imagery, commercially purchased datasets etc.), the actual production data stores (ex: *Structured Observation Management (SOM), Aeronautical Migration System (AMS), etc.) and NGA products (Digital Nautical Chart (DNC), Intel Reports, Geodesy Models, Navigation Planning (NAVPLAN) Charts, Fleet Guides etc*.). This is "the content".
- **Activity Data:** This is the data other than mission content, needed to make an activity/service run. This includes code, configuration files, logs, etc.
- **Analytical Data:** This is the ephemeral working data/products that Analysts are analyzing on their desktops or in an Analytical Tool/Service. It is not considered Mission Data until it is finalized/published to the gold repository and/or the customer. The published product created from the results of Analytical Data are also "Mission Data".
- **Corporate Data:** Data used at the enterprise level that enables the business of NGA but is not directly part of the mission. This would include PeopleSoft Data, Identity and Access Management (IdAM) data, Personal Identifying Information (PII), financial systems and other Enterprise needs, workflow and process tools.
- **Organizational Data:** This is the data needed for the business process of individual organizations. This would include things like International Standards Organization (ISO) processes, Org Charts, briefings… the types of things organizations generally put in their shared organization drives now.

2.1.7 Content ID (REVISED!)

Content ID is a way to categorize a related set of data, for example: “Digital Nautical Charts” or “Absolute Gravity Survey.” Mechanically, a Content-ID is a unique identifier created when a logical set of data is registered in the Data Inventory. Each data set identified by a Content ID has a Data Custodian, a Data Steward, Retention/Lifecycle policies, access control policies etc. The Content ID is used to track data throughout the migration process. Virtual Folders within S3 Buckets are created based on Content ID, and access control and lifecycle policies are then applied to those Content ID Virtual Folders based on the rules for that logical set of Data registered in the AR. Please Reference the Data Movement Process (section 3.3) and the Data Migration Checklists[39] on how to get a Content ID for your data and move it through the migration process.

2.1.8 Roles

Data is acquired, managed and provisioned through various roles (see Table 3 below).

Table 3: Data Services Roles

UNCLASSIFIED	
User Title	***User Role***
NGA Chief Data Officer (CDO)	Responsible for Data Governance at NGA in general, and for the CDO-established NGA Content Account(s) on C2S in particular. The CDO must ensure that the NGA Content Accounts are properly maintained and configured. As the owner of the C2S CDO Mission Data and Corporate Data accounts, the CDO must approve any new Data or Data Services being added to the Account(s). The CDO also covers direct data migration costs, to move data to the cloud.
Data Custodian	Responsible for bringing the data into the agency. Often known as the Data Owner, this might be the person who: • authorized the expenditure of funds to buy a set of data • authorized an Analyst to retrieve a set of free data • approved a deal with a host nation or other entity to obtain data • is in charge of the group that produces the data/product One way or the other, he/she is the person, with the authority, that is responsible for that set of data at NGA. The Data custodian is responsible for the ongoing maintenance of his/her data. This includes budgeting for storage costs (including in the Cloud), paying storage bills, setting retention policies on the data, and making sure data sets are kept up-to-date or retired as appropriate. Data Custodians must approve of every Data Set belonging to them being migrated so that they are aware of the scope of their data and can execute their responsibilities.

[39] Cloud Data Migration Step-by-Step Checklist, *CAMG 2016.*

User Title	*User Role*
Data Stewards	Charged with making all information collected and all analysis produced by an IC element available for discovery by automated means by authorized IC personnel[40]. In doing so, they: • Define and manage access and handling policies for their data set so that the data is treated in accordance with applicable legal and policy constraints. • Issue Data Management instructions throughout the data life cycle. • Determine if the existing cloud services provide access control mechanisms that meet their security needs.
Data Technical Staff	Perform technical actions on behalf of the data steward. For example, they may prepare and route data to its intended destination in the desired format with appropriate Smart Data labels applied. Or, perform metadata tagging research.[41]
Data Knight/Champion	Often the person delegated to attend the DMWG and coordinates with the Data Custodians and Data Stewards in their organization to answer data related inquiries.
Activity Data Manager	This role is assigned to one or more Activity automated systems, not a specific user. Gives authorized system users rights to manage (Create, Read, Update and Delete) that Content on behalf of the Data Custodian. Systems that are not Activity Data Managers will only be given Read access to data. For example, the AMS Activity is the assigned Activity Data Manager for the AMS Database per the AMS Data Custodian. If AMS were not, the AMS software could not be used to insert, update and delete data in the AMS database.
Cloud I&A PMO	The Information and Assurance Program Management Office (I&A PMO) Coordinates migrations, and specifically tasks DSP and ISP, including generation of task CRQs. Controls the actual execution of the data migration once the DMWG has approved it.
Data Scientists	Determine the relevancy of data with respect to mission need and investigate and prototype data analytic approaches to yield useful analytic conclusions from one or more IC data sources. They may provide input into the indexes, extractions, or correlations to be performed against their submitted data. Note that this role is intended to also cover roles of other IC users (e.g., data specialists, developers) who perform similar activities aimed at extracting knowledge from data.
Developers	Design, develop, and implement services and data flows to support needs.[42] They interact with/use other services to develop, integrate, and deploy capabilities. May also be known as software solution engineers and by other terms.

For example, consider the NGA Aeronautical Safety of Navigation group (SFA) DAFIF. A DAFIF Program Manager is in charge of the product line. The Mission Data Custodian for

[40] IC Directive Number 501, Discovery and Dissemination or Retrieval of Information Within the Intelligence Community

[41] Defined in ODNI ES 00594 as “An organization that is responsible for executing data-related tasks on behalf of an Originating Element. These tasks may include collecting, tagging, and processing data.” Note that the Data Custodian organization may be different than that of the Originating organization

[42] Intelligence Community Information Technology Enterprise (IC ITE) Data-Centric Management Principles, V 1.1, 14 February 2014

DAFIF would be the head of SFA, and the DAFIF Program Manager would be the Data Steward.

2.2 Guidance from the CDO

The NGA CDO has issued the following Guidance with respect to Data in the Cloud.

2.2.1 General Guidance

Guidance: All data will be managed in accordance with NGA Data Management, retention and records management policy

Data Stewards and Data Custodians will set lifecycle rules on their cloud data repositories. Those lifecycle rules will follow National Archives and Records Administration (NARA) guidance and will indicate when Data/Files/Objects can be moved to a near-line archive, and when they can be moved offline. Electronic Records Management metadata tags will be applied during conditioning to allow for effective records management.

NGA Data Management policies shall be followed, as documented in the NGA Data Management Guidance and Unified Data Strategy.[43]

Guidance: Data services built for the cloud shall be delivered suitable for use as enterprise services whenever applicable

Conditioning, data load, data access and other data services for applications built for the cloud that may possibly have general utility are to be delivered so as to be technically suitable for use as enterprise services.

Guidance: Encrypt Data at Rest (DAR) and Data in Transit (DIT) (see Annex I: Cloud Security Section 6.1)

Data at rest (DAR) and data in transit (DIT) across and between cloud environments will be encrypted. NGA follows DoD Cloud Computing (CC) Security Requirements Guide (SRG) v1r2, NIST 800-53, and CNSSI 1253, all of which provide guidance for DIT/DAR. An Analysis of Alternatives (AoA) has been conducted by NGA TAEO Security Engineering to evaluate encryption and key management solutions. The results of the AoA are in analysis and the solution will be identified through the NGA acquisition process. Annex I: Cloud Security, addresses enterprise security services across UAWS, SC2S and C2S; section 7.4 incudes encryption solution details.

Data Encryption for Unclassified Commercial Cloud (U-AWS): The U-AWS will store, process and transmit both Public Releasable Information and Controlled Unclassified Information (CUI) data (i.e., LIMDIS). The U-AWS will be accredited to process up to Impact Level 4 data. The DoD CC SRG v1r2 requires that 1) for all Information Impact Levels, encrypt all Data at Rest;

[43] NGA Data Management Guidance, 2016; and, NGA Unified Data Strategy, 2015.

and 2) for (CUI) data, use a FIPS 140-2 (minimally Level 1) encryption solution.

Data Encryption SC2S and C2S: The Secret Commercial Cloud Services (SC2S) and Commercial Cloud Services (C2S) encryption solution for DIT/DAR will be accredited in accordance with ICD503. An objective of the aforementioned AoA is to implement an enterprise encryption solution across UAWS, SC2S and C2S.

For additional information on DIT/DAR, please see Cloud Security Guidance, Section 3.3.4.

2.2.2 Mission Data Guidance (REVISED!)

Guidance: Data belongs to the NSG community

Data does not belong to a specific group or program, but to the National System for Geospatial Intelligence (NSG) (including all IC) community as a whole. Data will be shared unless restricted by access or policy. Data access will be determined by the access associated with data itself and the roles and permissions of those attempting to access the data, following NGA releasability policies. The role “data steward” does include marking and otherwise associating access and interpretation rules to the data, but a data steward should not support actions that would restrict access by an authorized user with a need to know, even if the user or use was unanticipated.

Guidance: Metadata tagging minimum standards are enforced automatically

Conditioning and validation processes will be part of the workflow; items that fail (e.g., are deemed to have insufficient handling information or to be not-discoverable) are so indicated by status metadata or are routed to separate areas (“dirty buckets”). The minimum standard NGA will follow is dictated by the Intelligence Community Enterprise Data Header (and its dependencies) coupled with applicable NSG Metadata Foundation (NMF) Core elements. Additional fields to handle Records Management are also mandated but are not necessarily considered for minimum access and discovery capabilities.

Trusted Activities, such as those designated as Activity Data Manager, will have direct access to the data whether it is clean or dirty. Access to “dirty” data is necessary to a) get the data conditioned and b) enable legacy programs to continue operating while conditioning is taking place. Data must be conditioned before it can be discovered by everyone else.

Metadata tagging, Identity and Access Management, business rules (that define relationships between data attributes and user credentials); and Policy Enforcement Points (negotiate access and releasability) enable a strengthened data security posture.

Guidance (*NEW*!): Mission data access is permitted in accordance with *responsibility to provide* principles while enforcing all necessary access controls.

This is to be achieved to the extent possible using automated means matching attributes and groups detailing data restrictions and user entitlements. Specifically, Entitlement attributes such as Clearance and Special Access permission group or role membership or non-membership must be explicitly asserted and tested, including:

- Data are tagged with metadata that have classification, dissemination controls and access group information with associated entitlements policies.
- User identities are tagged with metadata that has clearance, role and group membership information with access and dissemination consequences.
- Methods, rules and services exist to automatically test data access criteria against access attempt credentials, in accordance with policy.

Access Groups and roles can be created at any broad or fine level of detail, by category, by inclusion, by exclusion, or by specific itemization (e.g. listing who what and when).

Guidance: Mission Data must be approved before migration

Before any set of Mission Data can be migrated to C2S, the CDO, the Mission Data Custodian and the Mission Data Steward must approve (by electronic signature) the set's migration. If no one claims ownership or provides stewardship of a set of Mission Data, that data will not be migrated. If the Mission Data are deemed no longer relevant or active, then the Mission Data Custodian or Mission Data Steward (or CDO) may choose to not migrate the data (which then would fall under NARA records management rules including potential disposal or archiving). The approval is only needed for the initial migration, not new updates or additions to the existing data set.

Guidance: Mission Data will be migrated to C2S/AWS

C2S/ Amazon Web Services (AWS) shall be the default storage location of all NGA Mission Data.

If IC partners request NGA Data on the IC-GovCloud for Analytical purposes, a copy of the data requested can be made available at the requested location. IC-GovCloud usage may be allowed for other special reasons to be evaluated on a case-by-case basis.

Guidance: Mission Data will be stored under a NGA Content account

All Mission Data/Content shall be stored under the NGA Content Mission Content account in C2S, managed by the CDO. This underscores enterprise data ownership and helps guarantee uniform accessibility while maintaining necessary stewardship and access controls. A system/program, group or individual may still have a separate C2S account with any permissions necessary. Within the NGA Content account, numerous different databases, Archives, S3 buckets, and other data stores can be created, and managed, with the appropriate permissions and roles. Those data stores can then be accessed by the appropriate activities that are external to the NGA Content account.

Guidance: Mission Data will be cataloged for discovery and exposed via services

Activity owners/designers should work to maximize discovery and the potential for reuse. Specifically, they shall maintain and catalog metadata that describe Mission Data, such as the EDH and the information contents of the Trusted Data Format (TDF), including provenance and access information (further detailed in the Metadata section below). Whenever practical,

application data queries will be encapsulated as services exposed to the community and published in the service registry (TBD 003).

Guidance: Mission Data will be managed with integrated security and access control

The NGA Cloud implements multiple layers of defense, or defense-in-depth, to protect against unauthorized accesses and introduction of vulnerabilities into the NGA environment. The Cloud infrastructure is protected by packet analysis, data loss prevention, auditing, privileged access management, and encryption for data at rest and in transit. In addition, various other security services are employed to provide extra layers of protections for the environment. Data Stewards and Data Custodians will leverage PKI, IdAM, role-based access control (RBAC) and PEPs to allow secure access to data and metadata.

2.2.3 Activity Data Guidance

Guidance: With the exception of Logs, activity owners/designers determine the most suitable activity data storage type and location.

See the C2S Storage Whitepaper[44] for a discussion of options. Security and audit files will be accessible by qualified security administrators only; see Annex I Cloud Security for additional information

2.2.4 Analytical Data Guidance

Guidance: Analytical Data will be stored as determined by owners of the enterprise analytical services and exploitation services.

Best practices suggest that most analytic data should be dynamically compiled in cache if practical, or in temporary data structures, such as Hadoop, and automatically deleted at the conclusion of the analysis. Certain analytic situations will require other patterns, at the discretion of activity owners.

2.2.5 Corporate Data Guidance

Guidance: Corporate Data are Access-Controlled

The NGA Corporate account (established by the CDO) will have protections in place to address security controls for Personally Identifiable Information, finance, Human Resource and other sensitive non-mission data types. Security measures such as RBAC, PEPs and business rules will be employed to control access to both discovery metadata and data content.

Guidance: Corporate Data will be migrated to C2S

The CDO has specified that C2S will be the storage location of all NGA Corporate Data.

[44] Design Whitepaper, Cloud Data Architecture Structure Choices.

Guidance: Corporate Data will be stored under a CDO-established NGA Corporate account

All Corporate Data/Content will be stored under a CDO Corporate Content account in C2S. This underscores enterprise data ownership, providing uniform accessibility while maintaining necessary stewardship and access controls. A system, program, group or individual may still have separate accounts with any permissions necessary. Within the Corporate Content account, numerous different databases, archives, and other data stores can be set up, and managed, with the appropriate permissions and roles.

Guidance: Corporate Data will be cataloged for discovery and exposed via services

Corporate Data Custodians shall publish discovery metadata in a Corporate Metadata Repository distinct from the Mission metadata repository. Whenever practical, application data queries will be encapsulated as services exposed to the community and published in the service registry.

Guidance: Corporate Data will be managed with integrated security and access control

The NGA Cloud perimeter implements multiple layers of defense, or defense-in-depth, to protect against unauthorized accesses and introduction of vulnerabilities into the NGA environment. The Cloud infrastructure is protected by packet analysis, data loss prevention, auditing, privileged access management, and encryption for data at rest and in transit. In addition, various other security services are employed to provide extra layers of protections for the environment. Data Stewards and Data Custodians will leverage PKI, IdAM, RBAC and PEPs to allow access to data and metadata.

2.2.6 Organizational Data Guidance

Guidance: Organizational data currently on a shared drive and/or SharePoint will be automatically migrated to the equivalent NGA enterprise location in the cloud.

No specific, individual organizational actions are needed at this time; data stewards may relocate this data at their discretion.

2.3 Data Inventory (Revised)

The Data Inventory in the NGA Architecture Repository (AR), established in 2016, contains the consolidated information collected about NGA data. An AR inventory data dictionary is available.[45]

[45] Data Dictionary for AR Data Inventory.

Check the status of your data in the AR Data Inventory here:

http://ndegsnarwvapp01.titanium.rttitanium.nima.ic.gov:8082/ee/request/folder?id=55216

No login is needed. Enter as Guest.

The Data Inventory is a one-stop shop for data information at NGA. It contains:

- Data Status Information: Data Status, Migration Status
- Basic information: Name, Description, Category and Classification of the data
- Custody: Organization it 'belongs' to and Point of Contact (POC)
- Storage information: data storage network(s), type of data, method of storage and data size
- Relations: Production, Dissemination and Consuming activities (systems) that use, produce or host the data.

To view all the information available on a given data set, one can either go into that specific record in the AR or download the Authoritative GOLD copy spreadsheet and see it all in one view. New functionality will be added over time.

The data inventory is continuously updated. Every migrating Activity must provide this critical information to allow for a successful migration. Data will not be stored in the cloud unless the CDO and/or Data Custodian sign off. Continued effort is required by NGA data stewards to ensure the completeness and accuracy of this information.

3 DATA MIGRATION

3.1 NGA Migration Background

At the end of calendar year 2015. the NGA Deputy Director, Ms. Sue Gordon, issued a mandate[46] to migrate all content and activities to the cloud by the end of calendar year 2017. To date, NGA's approach to this mandate is to migrate each PoR individually. The CDO plans to migrate the mission data ahead of the activities for customer consumption and PoR testing, as well as interim and final operations. Data needs to be migrated before the activity to accelerate customer consumption, activity test readiness and interim operations. In either case, as shown in Figure 3-1, migration is dependent on both the data and activity migration.

[46] https://ngaonline/sites/CIO-T/InformationCenter/Documents/Publications/U-2016-00069-ACTION-CLOSED.pdf

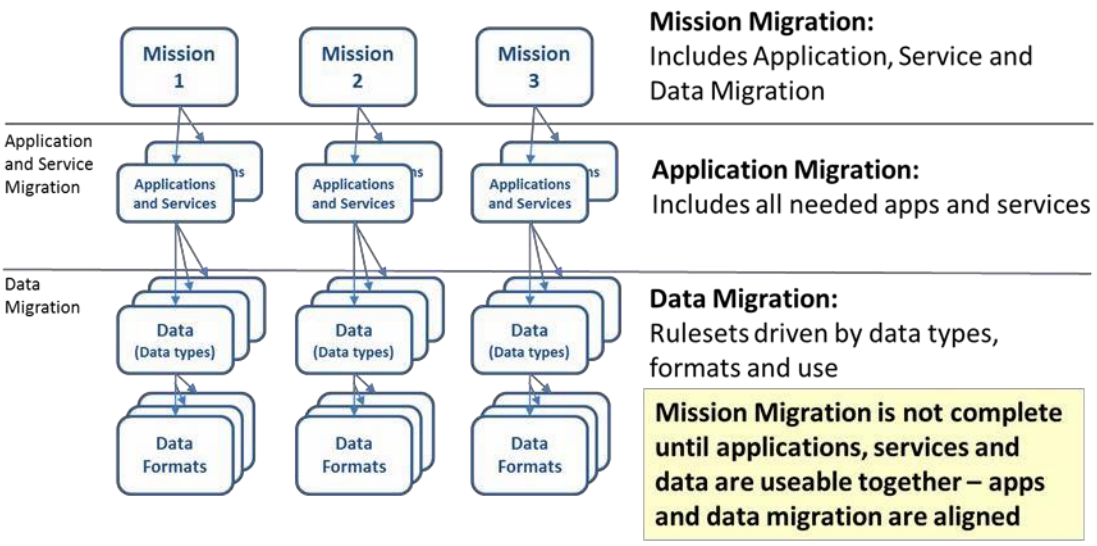


Figure 3-1: Cloud Migration Dependencies

NGA has multiple objectives for migration:

- Do not break mission capabilities,
- Get off the current infrastructure,
- Obtain secure, efficient, intelligence integration.

3.2 Data to the Cloud Process (REVISED!)

This section outlines general steps to identify content, approve requests and create/implement cloud change requests that will apply to most data sets. This process applies to moving data to the cloud, establishing storage in the cloud with the appropriate accesses, and creating data feeds. Each data set may have unique issues and considerations. Cloud migration preconditions are:

1. A Data Custodian (also often called 'Data Owner") must be identified,
2. The Data must be registered in the Data Inventory such that a ContentID is associated to the data, and
3. Essential metadata (a minimum set) must be populated for the particular data set.

A *Cloud Data Migration Step-by-Step Checklist*[47] is maintained separately, since it is often updated.

[47] *Cloud Data Migration Step-by-Step Checklist, CAMG 2016..*

It is included in this document by reference

This process is the same for both file/object based data and database data with a few exceptions; database data will not be posted to a dirty bucket, but instead to its designated database structure. While the ISP and DSP will move database data, as the move file/object data, it will be up to the ASP to ETL data into the new database in the cloud.

3.2.1 Phase 1: Identify Content *(REVISED!)*

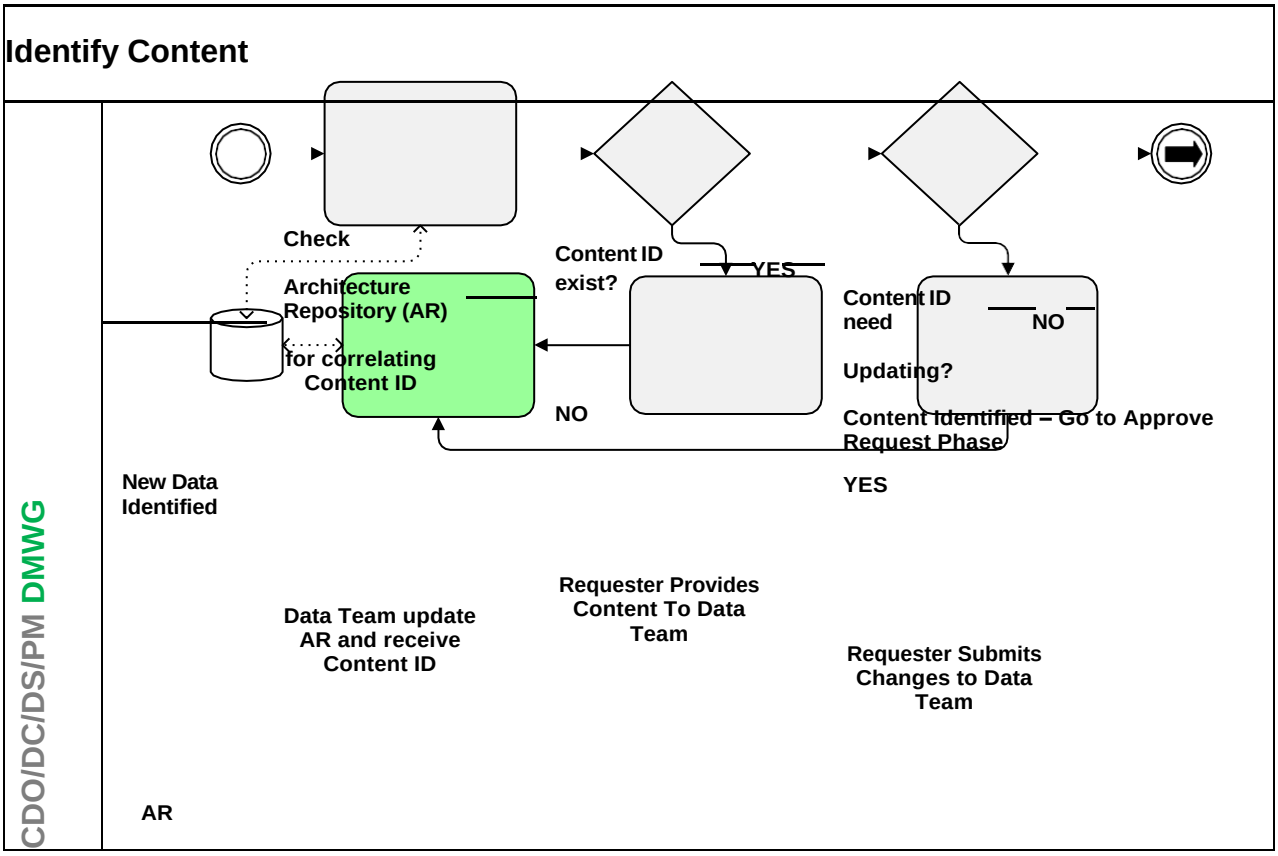


Figure 3-2 Phase 1 - Identify Content (assign Content ID)

(U) This phase begins when a party (Chief Data Officer (CDO) Data Custodian (DC), Data Steward (DS), or Project Manager (PM)) identifies data to be migrated to or established in the cloud.

- As shown in figure 3-2, all parties must check the Architecture Repository (AR) Data Inventory to see if their content aligns with any content already cataloged.

- If their content is not found the initiating party must fill out the **New Data Form**, following the instructions in the **Cloud Data Migration Step-by-Step Checklist,** to update the AR and receive a Content ID.
- If the requester finds their Content ID(s) but any of the metadata is incorrect, the requester submits changes to the Data Team.
- (It is important to note that at this point there must be one Data Custodian identified for the Content ID. Data Custodians can own multiple Content IDs but only one Data owner can be identified per Content ID.)

3.2.2 Phase 2: Approve Request (REVISED!)

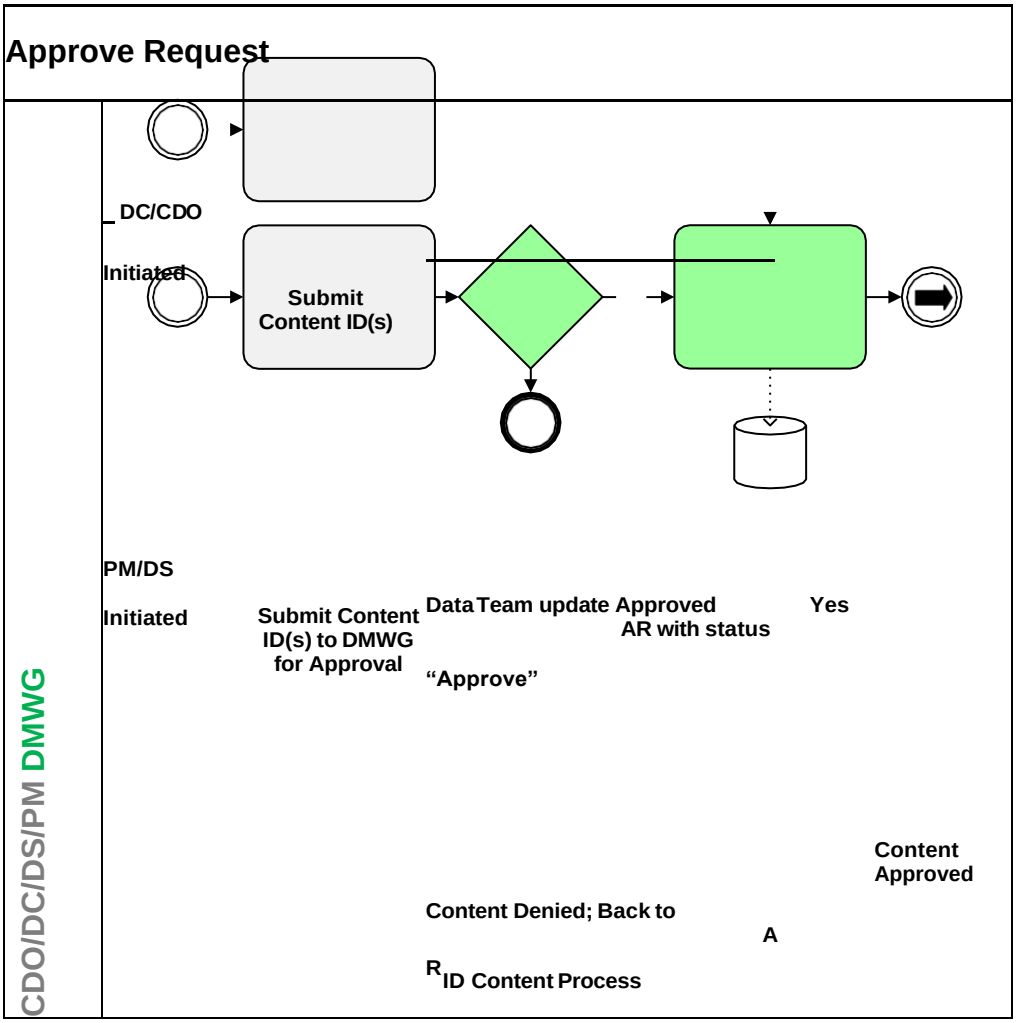


Figure 3-3 Phase 2 – Approve Request

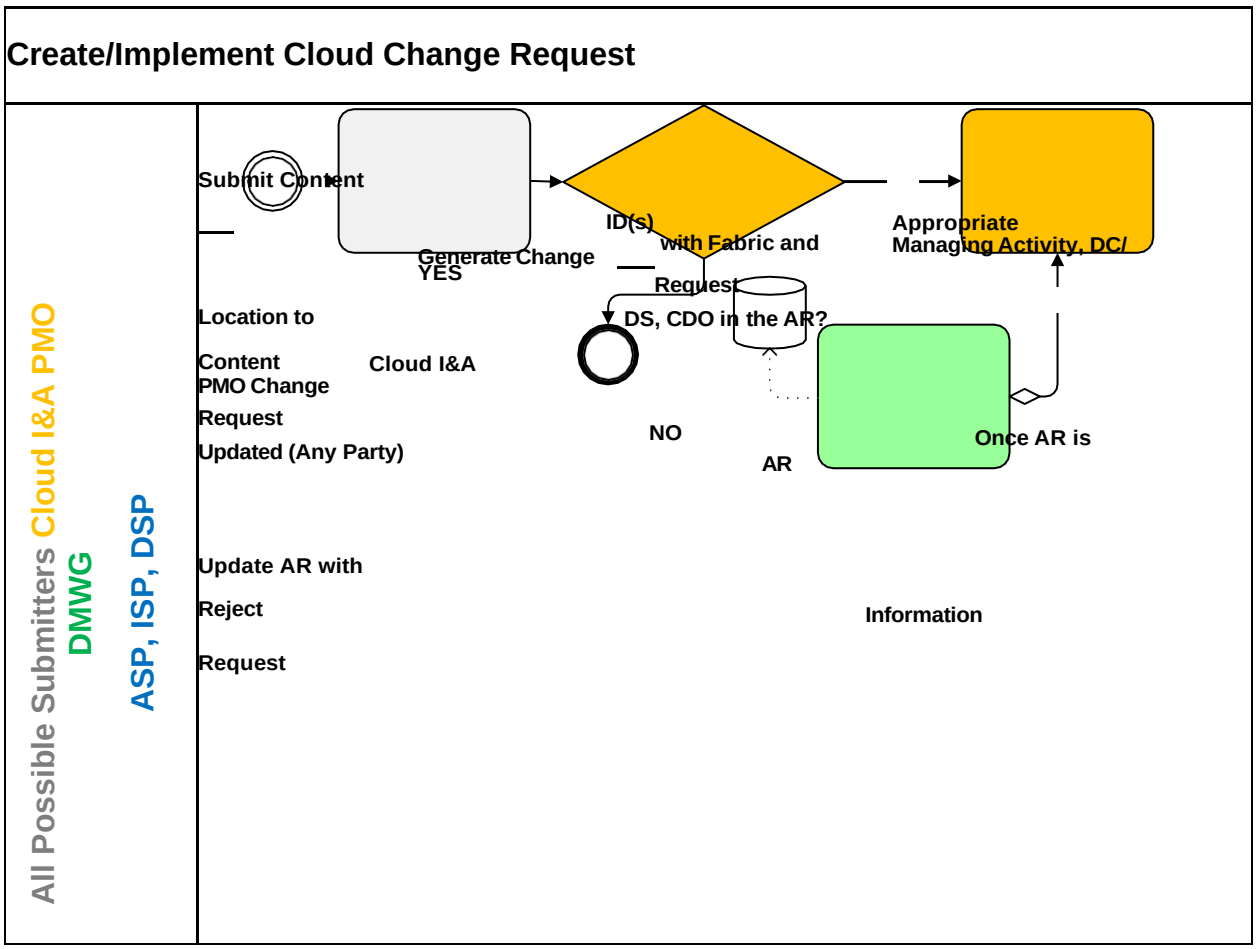
(U) This phase begins when the CDO/DC/DS/PMs compile and submit their particular content ID(s) for approval (for migration, data feed set up, create storage and access for repository

space, etc.).

- The DC for the particular Content ID(s), as a representative(s) of the Data Management Working Group (DMWG), reviews approval requests.
- Content IDs are checked, and AR information is verified by the DC and Data Team. Additional data, if missing, may need to be collected at this time.
- Whether the content is approved or denied the AR is updated by the Data Team to reflect the approval status of the data (for migration, data feed set up, create storage and access for repository space) that is correlated to the Content ID.

- (Note: If the CDO or the DC submits the data for approval, the DMWG is bypassed and the AR is updated by the Data Team to reflect approval and additional information if needed.)

3.2.3 Phase 3: Create/Implement Cloud Change Request *(REVISED!)*



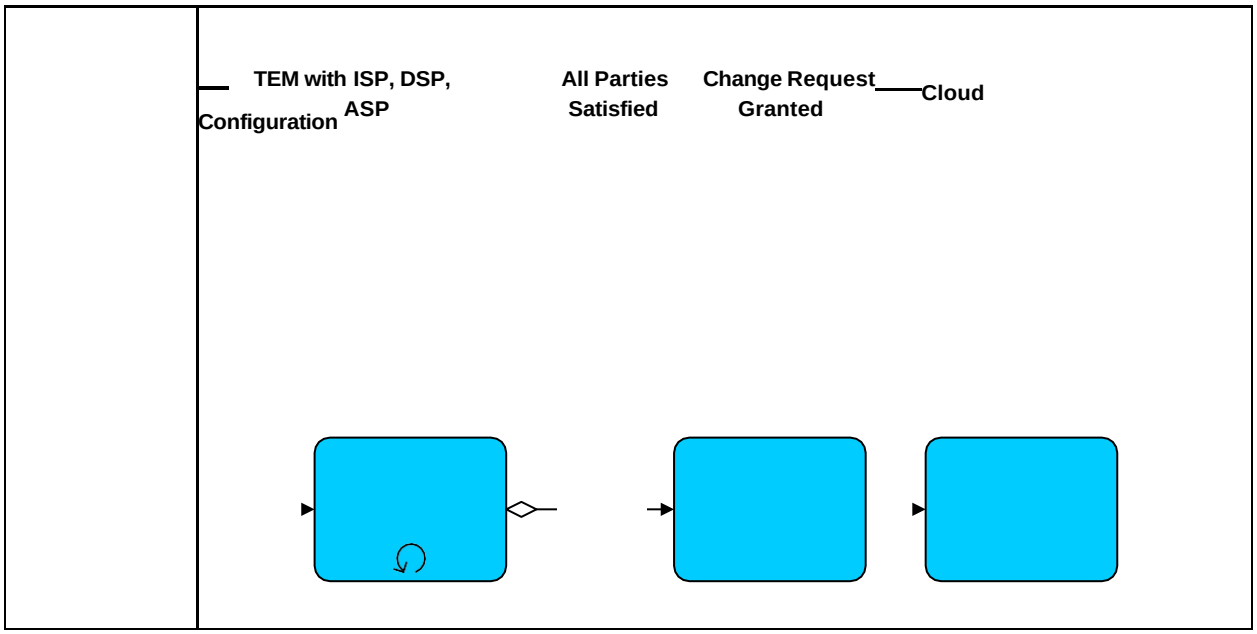


Figure 3-4 Phase 3 – Create/Implement Cloud Change Request

(U) This phase begins with all submitting parties (the CDO, DC, DS, PM or representative) submitting to the Cloud I&A PMO, a request to move, create storage and access for, or create data feed for a set of one or more content ID(s) that was already approved out of Phase 2. The Cloud I&A PMO verifies that this request is coming from the appropriate managing activity, DC/DS, or the CDO for the content ID, else the request is rejected. A change request is generated then TEMs are scheduled for the ISP, DSP, and ASP. After the details are worked out the request is granted (data moved, storage created, data feed set up, etc.), the AR updated, and tools are pointed to data's new location in the cloud.

3.2.4 Conditioning for File/Object based data (REVISED!)

The Metadata Guidance in section 4 has additional details on Data Conditioning. This section provides a high level overview of steps following the data movement process.

All data needs minimum metadata (specified in Appendix H, which includes the GUIDE ID) to be discoverable and accessible by the enterprise. The process of defining and adding this metadata is called "Conditioning". If the minimum discovery and access metadata is not immediately available when the data is moved, the data is placed in a logical 'Dirty Bucket' and further conditioning is scheduled.

There are many ways to go about conditioning the data.

1. Originating Activity Data Conditioning: In many cases, only the Originating Activity will have the information and tools needed to condition the data. In these cases, the Activity should submit the metadata along with the actual data files, as part of the data

movement process. Once the initial migration is completed, to support ongoing operations, the information and expertise must be embodied into an Enterprise Conditioner Service.

2. Enterprise Conditioner: In some cases, there is an Enterprise Conditioner already created for the file type of the data you are migrating. In this case, the Data Steward would be responsible for running the Enterprise Conditioner after the data is migrated.
3. In some cases, information needed to condition data is not stored in any digital way – the Data Steward will be responsible for transferring that corporate knowledge to the metadata catalog.

If there is no Enterprise Conditioner, and the required metadata cannot be provided by the Originating Activity, then the Data Custodian needs to approach the CDO via the DMWG with the request to create a conditioning tool. The CDO office will work with the Data Custodians on prioritization of conditioning tools and strategies to create the tools in alignment with Mission Needs and Timelines.

3.2.5 Conditioning for Databases

At this time, so as not to break legacy functionality, no changes will be made to the database internal schemas. The Conditioning for Databases will be the registration of all the Web Services associated with that database in the Enterprise Service registry and populating any mandatory metadata there.

3.3 Production Components

The final production architecture will be composed of Catalogs and Registries for all domains, file-based content where the content is persisted on the originating domain, and non-file-based content that is either in an interim or final operational state. Figure 3-5 identifies the different data components. The definitions of each are found in Appendix A.

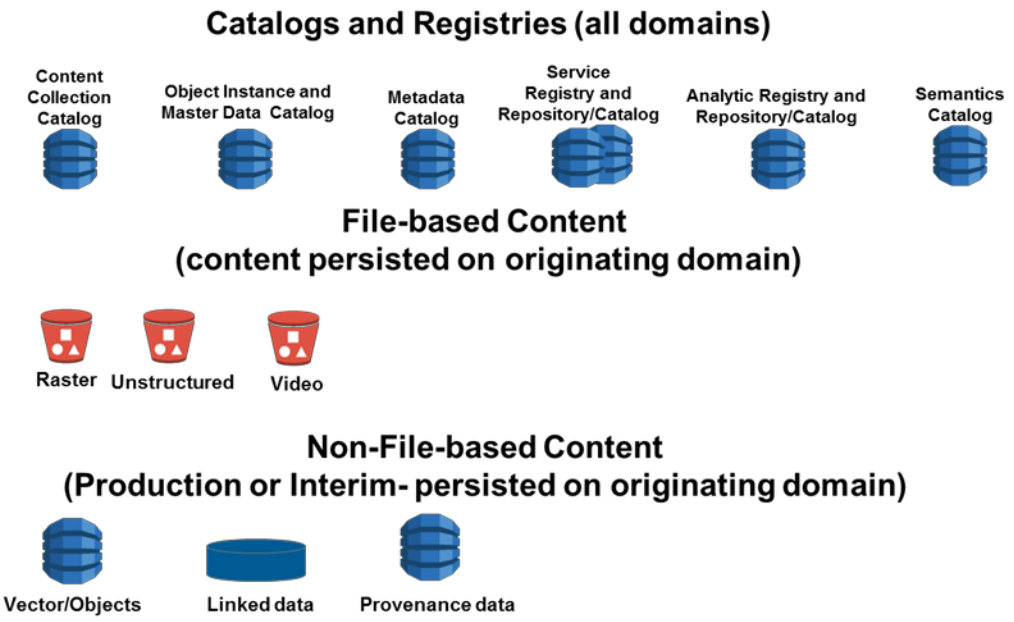


Figure 3-5: Production Architecture Components

3.4 Data Migration Guidance

The following guidance shall be followed in migrating data to the cloud:

Guidance: Do not mix any data in the staging architecture that is not mixed today.

Guidance: Provision staging S3 buckets by source, data type and classification.

Guidance: Provision additional buckets as needed – for Domestic and Special Access Program (SAP) data.

Guidance: Provision a ‘Manual Review Dirty’ bucket per migrating system for all source data without appropriately tagged metadata.

Guidance: No end user access to the ‘Manual Review Dirty’ bucket. Data steward must be given access to remediate the content and workload managers must have oversight permissions.

Guidance: Migrate non-file-based data AS-IS following database criteria guidance.

Guidance: Grant ‘interim’ operational access if content is not in desired organizational structure.

Guidance: Easy-to-tag legacy data may skip the staging ‘Dirty bucket’ phase if conditioned and properly tagged.

Guidance: Policy Enforcement Points (PEP) enforce user access to all data stores – via a service or view, no direct access.

Guidance: Synchronization between legacy and cloud stores may be needed until services are migrated and legacy can be retired. Synchronization is a legacy responsibility. Parallel operations may be necessary until the legacy system can be shut down.

Guidance: Consider resiliency requirements for production storage; e.g. multiple availability zones for operational data.

Guidance: Implement S3 Bucket Strategy

- Standard Enterprise S3 Buckets are predefined (42 to date, see Appendix J for details).
- Content-IDs assigned to data at the logical dataset level (~795 Content-IDs currently registered in the NGA Data Inventory).
- Virtual Folders are set up for each ContentID within an S3 Bucket, managed by Activity Data Manager.
- Lifecycle/Data Retention rules set at the ContentID level.
- Permission for direct S3 Bucket Access by Trusted Activities set at the ContentID Level
    - Read Only access by default
    - Write/Delete access (Activity Data Manager) requires ContentID NGA Data Custodian approval
    - Trusted Activities, if not using the Enterprise PEP, are responsible for ensuring appropriate access by Users.

S3 Bucket naming standards are presented in Appendix J.

3.5 Cloud Migration Lessons Learned

The feedback loop can be a valuable aspect of migration management. Cloud Migrations Lessons Learned are captured in the NGA Lessons Learned Portal, shown in figure 3-6 and found at this site.

https://ngaonline/sites/oso/osop/LessonsLearned/SitePages/CloudMigration.aspx

The Lessons Learned portal represents an industry best practice. It is a way to see and avoid the pitfalls experienced by others in their migration efforts. It is also an opportunity for groups to provide feedback to the CAMG teams and affect future Cloud Guidance revisions.

4 CLOUD METADATA GUIDANCE

4.1 Cloud Metadata Summary

NGA Mission Data have historically been difficult to manage. From ingest to dissemination, Access, Discovery, and Retrieval have been problematic, partly because of inconsistent metadata conditioning throughout NGA production pipelines. This document describes the initial concept for managing metadata in the IC Information Technology Environment (IC ITE). All NGA Mission Data will be stored in C2S; however, NGA will also push data to IC-GovCloud as appropriate.

Mission Data/Files will be submitted to a service that will condition the data. Once conditioned, Mission Data and metadata will be stored separately with data going to an Object Store and metadata going to a Metadata Catalog. Database-based data will not undergo direct conditioning. Instead, the service that manages that database-based data will be registered in the NGA Enterprise Service Registry (TBD-003) that has metadata that allows for its discovery.

Data conditioning requires two things: knowing the data, and a consistent way of describing data in a way that will be understood by human and machine consumers. To meet those requirements NGA will enforce metadata standards developed by the Director of National Intelligence (DNI) and NGA for data conditioning in C2S. Complying with the Trusted Data Format (TDF), Enterprise Data Header (EDH) and NMF standards will ensure that not only NGA data are discoverable in C2S but that NGA mission partners will be able to discover and use NGA Mission Data as well. Attached to this document are detailed breakdowns of the standards that NGA will enforce in C2S.

4.2 Challenges

4.2.1 Challenge #1: Increasing Discoverability of Mission Data

Historically, NGA has found making its Mission Data discoverable to the uninitiated user to be challenging. The consumers needed to know where to find their required data and products, typically by navigating a complex website to arrive at a tool that allowed them to download the needed data based on additional search criteria.

4.2.2 Challenge #2: Securely Sharing Information with External Partners

Legacy systems built for NGA and other IC agencies have implemented stove-piped architectures with their own proprietary access controls to protect mission data. This has hindered the sharing of information between agencies in the Intelligence Community.

Sharing information with non-IC agencies has also been problematic. If a non-US IC organization required access to data, and they were not eligible for access to all the information on a given network, a separate site had to be created for them to retrieve their data because it could not be automatically filtered. Posting data this way led to currency issues and duplicative storage.

IC ITE introduces enterprise security services to eliminate these proprietary access controls and provide a uniform method for accessing mission data from any agency. These services secure data at the object level. Redaction services used to filter content within an object are not included. NGA will supplement IC ITE's core security services with these capabilities. Access control decisions at the object level will be governed by DNI's IC CIO security specifications (e.g., the Enterprise Data Header). Objects requiring additional content inspection and filtering will be governed by NGA-specific metadata.

4.2.3 Tagging Mission Data to Overcome These Challenges

Tagging data with metadata specified by both the DNI and NGA can help improve discoverability and sharing of mission data in a secure fashion. By leveraging the cloud, enabling enterprise access controls, and enhancing and standardizing metadata, the following opportunities can be realized:

- Consistently metadata tagging data throughout the NGA production Process from Source Ingest to Product Dissemination
- Enable search of all NGA data through consistent metadata for NGA internal and external users
- Automated information release becomes possible
- NGA can inventory its own data and assess its overall enterprise value for enhanced sharing opportunities or opportunities to retire obsolete data based on usage statistics
- Automated data management at an Enterprise level becomes real. Appropriate metadata tagging provides for automated tools to enable decision making, therefore reducing the manual process of assessing data.
- Enabling Enterprise Level automation of high-to-low transfers
- Consolidation of disparate security services within the NGA Enterprise
- Solutions can scale for user and data access management

The NGA stood up the Office of the CDO to address data issues, among them metadata and discovery. Managing data as a true shared asset will greatly improve and indeed revolutionize the way NGA fulfils its mission.

4.3 CDO Cloud Metadata Guidance (REVISED!)

The CDO's mandate includes correcting the metadata/handling/discovery issues present in the current NGA architecture such that these issues do not persist in the Cloud. There are two broad categories of Mission Data: the "file/object" based data and "database" based data.

For file/object-based data:

- **Guidance:** All objects posted to the cloud will be conditioned.
- **Guidance:** NGA will use GUIDE.
- **Guidance:** NGA conditioned metadata will be stored in an NGA Metadata Catalog (TBD-002).

- **Guidance:** NGA will enforce DNI directives on using TDF[48] and EDH metadata standards for object conditioning.
  - **Guidance**: NGA will specify additional NGA Mandatory Conditioning Fields (See Appendix H) tags above and beyond DNI mandatory fields, as part of Mission Assertions.
  - **Guidance**: NGA will store the TDF and EDH metadata in the NGA Enterprise Metadata Catalog (TBD-002) instead of using the TDF as an object wrapper for persistent storage

For database-based data:

- **Guidance:** Web Services that expose database data will be registered in the NGA Enterprise Web Service Registry (TBD-003).

See also *Section 2.2.2 Mission Data Guidance* which addresses metadata tagging requirements for Mission Data Access and other purposes. These Guidance points are further discussed in the following sections.

4.3.1 All Data Objects Will Be Conditioned

In order to ensure full discovery, access, and retrieval, all NGA Mission Data files/objects will be conditioned. This conditioning allows for uniform application of metadata to all NGA Mission Data. Uniform metadata tagging provides for more autonomous data management procedures.

Metadata conditioning will resolve NGA data discovery shortfalls by attaching a well-defined set of attributes to all Mission Data files/data objects. These attributes, to include security markings, can then be cataloged and searched for every Mission Data Object in the NGA Enterprise. As a side benefit, this metadata catalog effectively creates an Enterprise Inventory for all NGA file-based Mission Data.

Conditioning is physically implemented in one or both of two ways. The first is referential, in which metadata are captured separately in a metadata catalog, linked to the object via Uniform Resource Identifiers (URI). The second is embedded, by which the metadata are included in a wrapper or envelope in which the actual object can be found, or directly in the object information. Multiple technical approaches are possible. It may also be mentioned that transport metadata are a different subject – TDF is an example of a transport metadata encapsulation protocol that can also be used for persistent storage.

NGA will be doing a referential implementation in a metadata catalog, not wrapping the files.

If every Mission Data Object is conditioned for ingest into the cloud, then this includes all incoming sources. When every piece of incoming source is conditioned then it is possible to

[48] TDF metadata subjects or fields, not the encapsulation protocol.

inherit the metadata from source to all products and datasets generated subsequently from said source, thus preserving pedigree and lineage.

With everything conditioned with the appropriate metadata it is possible to build automated PEPs to process and release data based purely upon a combination of Mission object metadata and consumer permissions as granted by the IdAM System. Some attributes identified in the IdAM System correlate to the attributes used in the EDH. Doing this reduces the need for excessive redundant storage and manual releasability processing.

The effectiveness of an enterprise IdAM System and data access management depends on the consistency of tagged data (compliance with standards).

The accuracy, consistency and robustness of data tagging is critical to support enterprise-based releasability and access control functions. The required enhancements to the security markings and metadata tags need to be identified to enable the programmatic enforcement of releasability rules and policies.

4.3.1.1 NGA will use GUIDE

The NGA will use GUIDE (Global Unique IDentifier for Everything) in accordance with DNI Standards for Intelligence Community Identifier. Application of the prefix defined in GUIDE will be required but registration with the community GUIDE is encouraged but not required. Information on GUIDE and GUIDE Services can be found at https://intellipedia.intelink.ic.gov/wiki/GUIDE. Note that for technical reasons, GUIDE is not recommended for use as an indexed key-ID field in some storage solutions such as S3.

4.3.2 NGA Metadata Will Be Stored in an NGA Metadata Catalog on C2S

NGA will establish its own metadata catalog to account for additional metadata beyond the IC Minimums stored within the IC-GovCloud. Since NGA will be storing all of its authoritative data in C2S it will stand up its catalog within C2S.

All ingested file/object Mission Data will be submitted to the NGA Conditioning Service. The NGA Conditioning Service will enable proper metadata tagging and then build a reference to the data. (During initial migration, conditioning may be performed by the originating activity). The actual data will then be sent to an Object Store(s) while the metadata will be sent to a Metadata Catalog as shown in Figure 4.

Handling data this way allows for uniform search and retrieval protocol, as well as provide a central location for metadata standards to be enforced. Note: Figure 4-1, is conceptual, not meant to represent actual design or implementation.

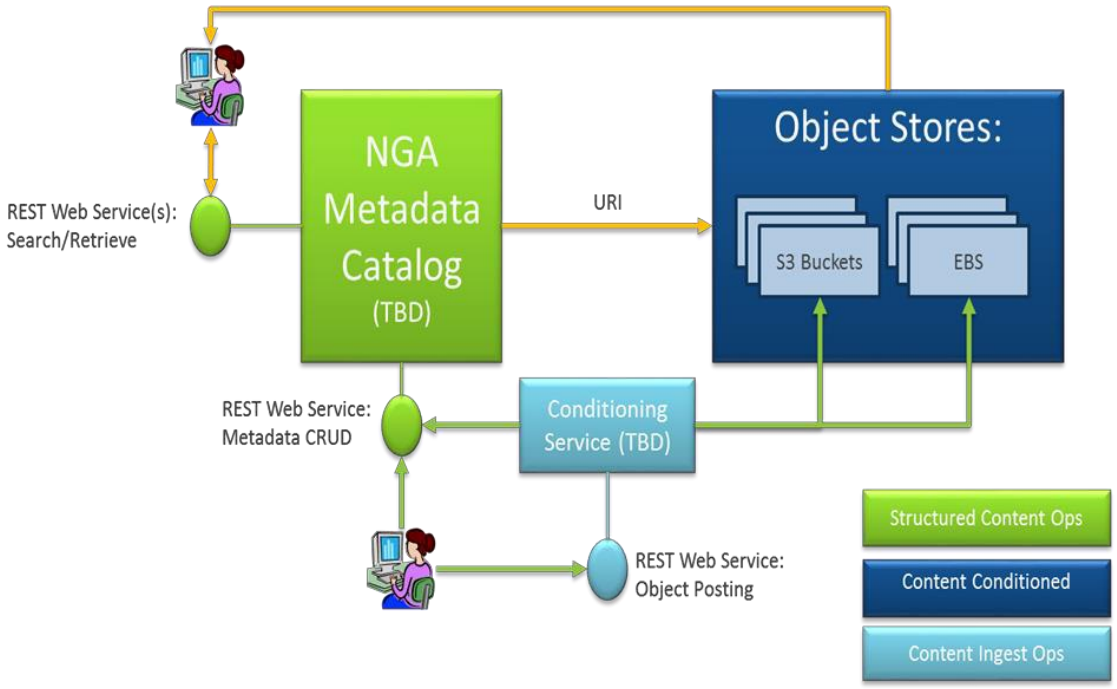


Figure 4-1: Concept: Metadata and Data in C2S

While the comprehensive NGA Metadata Catalog will reside on C2S this does not mean that NGA will not populate the IC-GovCloud metadata repositories. NGA will work with the IC to determine when and what metadata will be parsed and pushed from the NGA repository to the IC-GovCloud repositories. Figure 4-2 illustrates this concept.

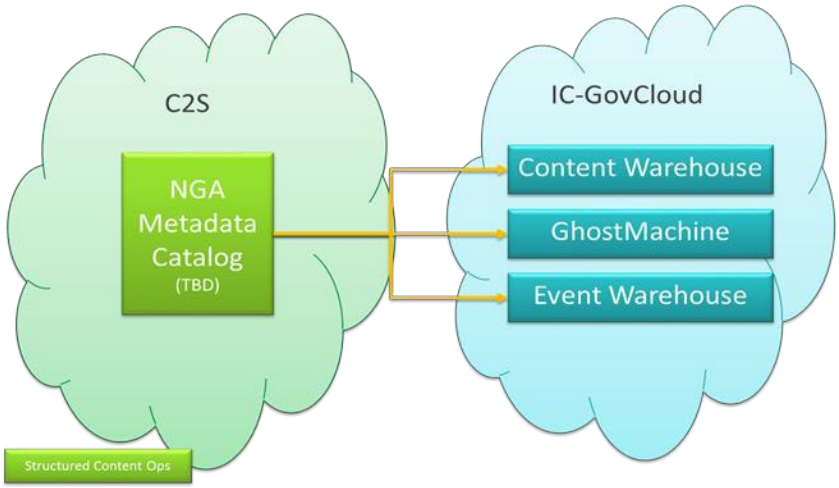


Figure 4-2: Concept: NGA to IC-GovCloud Exchange

There will be an NGA Metadata Catalog substantiated in the NGA unclassified cloud hosted by AWS Commercial.

4.3.3 NGA Will Use EDH and TDF

Intelligence Community Directive (ICD) 501 authorizes the DNI to produce and mandate metadata standards for the IC to adhere to in the Cloud. Following that, the DNI has published guidelines and specifications for the use of EDH and TDF to condition and standardize Mission Data for use across the entire IC. The NGA has traditionally followed the NMF to specify mandatory NGA metadata. The CDO has mandated the use of NMF mandatory content in concert with the EDH and TDF in the C2S NGA Metadata Catalog.

To comply with those mandates NGA has gathered information to aid content holders:

- The NMF has mandatory fields specified in NMF Part 1
- The A and S organizations have specified 24 fields in the NMF that they jointly consider mandatory (See Appendix E, Section E-2)
- The X Organization has submitted a list of discovery metadata that they require to the CDO. The question is “How do we reconcile the mandate to use EDH and TDF with the mandatory metadata from the NMF?”
- Step 1: Identify mandatory fields in TDF and EDH. (See Appendix G)
- Step 2: Identify the entire list of NGA NMF-based mandatory fields. (See Appendix E)
- Step 3: Cross reference the NGA NMF mandatory fields with the TDF and EDH. (See Appendix F)
- Step 4: Add Mission Assertions to EDH and TDF to cover NGA NMF mandatory fields that didn’t map and create a NGA profile of the TDF and EDH. (See Appendix H)

4.3.3.1 IC Enterprise Data Header (EDH or IC-EDH)

The DNI specification for metadata calls for use of EDH. The EDH is an enterprise data standard that was developed to support the Smart Data Initiative. It establishes a standard for universally and consistently applying a small set of metadata tags to any piece of data so that it can be identified, protected, tracked and handled throughout its life cycle within the enterprise, from creation to deletion. The EDH includes most Access Rights and Handling (ARH) attributes associated with an object. The ARH attributes must be taken into consideration for discovery, dissemination, and access authorization services.

Figure 4-3 is a graphical depiction of the EDH. EDH attributes and details are presented in Appendix G3.

Figure 4-3: DNI Graphical Representation of EDH

NGA will follow the published DNI specifications for all the boxes represented in Figure 4-3. The delivery mechanism is supported by the TDF.

4.3.3.2 TDF

NGA will follow the DNI specification of TDF metadata content. TDF exchange standard features a general container structure that encapsulates data objects and any assertions made against them. The TDF is an extensible, self-describing, self-protecting container/wrapper for assigning secure attribute assertions to any type of data. Figure 4-4 is a depiction of how the DNI conceptualizes the TDF structure. EDH attributes and details are presented in Appendix G2.

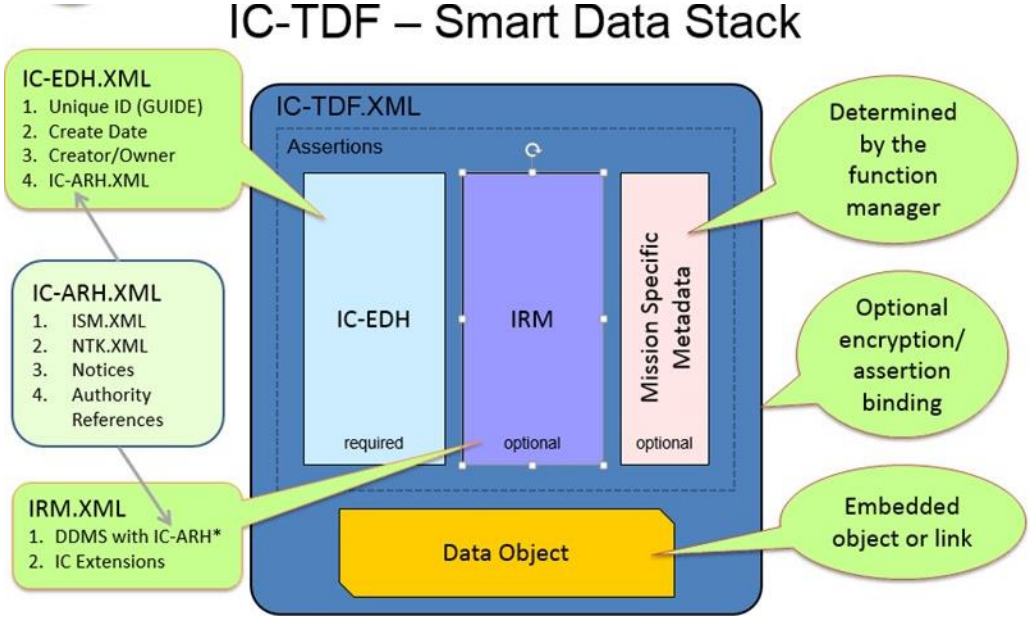


Figure 4-4: Graphical Representation of TDF

The TDF breaks down into to two main parts. The Assertions (metadata describing the Data Object) and the actual Data Object (Mission Data). Using the TDF allows NGA Mission Data to become Trusted Data Objects (TDO). Under that format, additional Assertions beyond EDH are made.

4.3.3.3 TDO (REVISED!)

A TDO is a wrapper containing a single payload. Each TDO requires at least one Handling Assertion at the package or metadata level (never encrypted), optionally a Payload Handling Assertion, optionally several Mission Assertions, and Payload.

- Handling Assertions explain who can use the content and to what ends. Typically, it is the Handling Assertions that are sent to the IC-GovCloud for IC usage. They are described, as a whole, as the EDH.
- Mission Assertions are only mandatory for the NGA Metadata Catalog on C2S. There are Office of the DNI published standards to inform content providers on what those are (See Appendix C: References).
- Payloads are the actual mission content/ data object. It can be a string, Extensible Markup Language (XML), or a reference to an external object.

4.3.3.4 Assertions

The NGA mandates several other assertions on top of what the EDH provides. This collective group of Assertions are known as Mission Assertions. These Assertions allow for a more robust set of access, discovery and retrieval attribution. These NGA/NSG Mission Assertions are specified in Appendix H: NGA Profile of TDF and EDH.

4.3.4 NGA Data Web Services Will Be Registered in the NGA Web Service Registry

NGA will take a different approach to database-based data. Instead of tagging every record, NGA requires that the web service that exposes that data to be registered in the NGA Web Service Registry (TBD-003) with appropriate metadata in the registry to make the service discoverable. Consumers can then search the NGA Web Service Registry (TBD-003) for web services that expose their desired content. Figure 4-5 is a graphical depiction of the NGA concept:

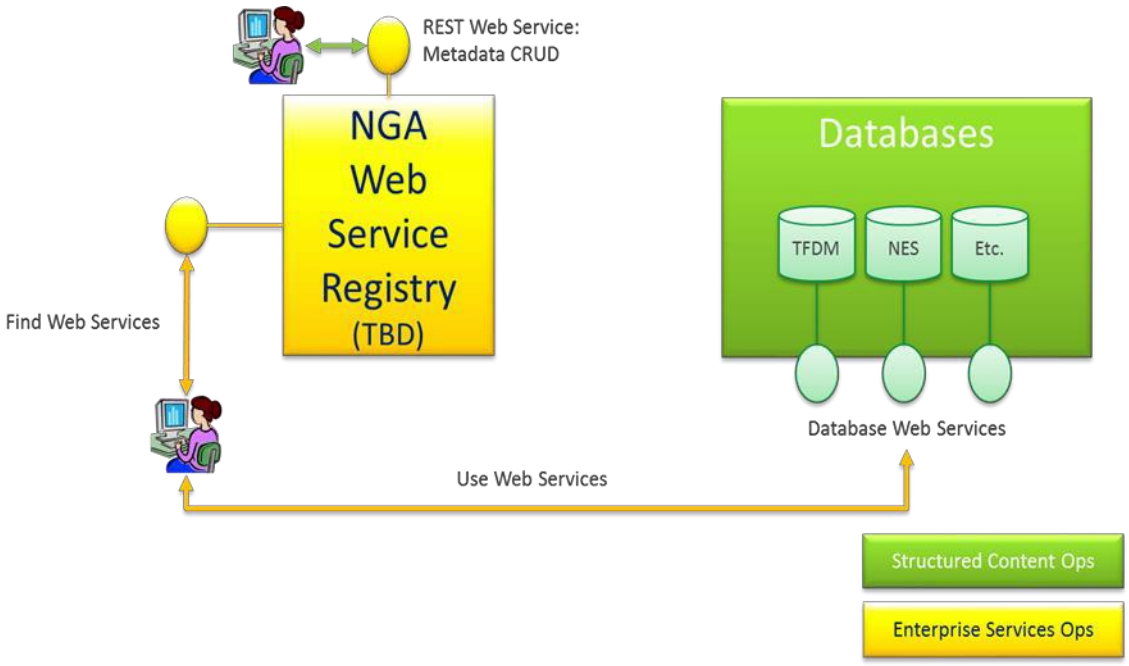


Figure 4-5: Concept: NGA Database-Based Discovery via Web Service Tagging

5 DATA ACCESS VISION (NEW!)

This segment of the guidance introduces Data Access concepts and then provides the current state of Data Access at NGA and the future vision of Data Access. In the past, data access has been system-specific and typically enforced as part of system access/login protocols, and often was not as fine-grained as desired or necessary. This guidance discourages a system-centric approach in favor of one in which data is managed independently of originating systems, and

access is automatically controlled by policies referencing attributes of the data and the user.

The concepts needed to achieve NGA and the future consistent IC-wide data access architecture end state and the capabilities desired are described in the sections below.

In alignment with DNI directives, the Data Access architecture for Mission Data has the following features:

- There is an automated way to discover and access data. All data is metadata tagged, personnel identities or roles are associated with accessibility attributes, and automated rules and processes will use these tags to automatically enforce accessibility and dissemination policy.
- *Responsibility to provide* is achieved. The default stance on Data is that it is shareable, within the classification and dissemination constraints as asserted by the security markings. However, *responsibility to provide* does not negate our responsibility to protect sources and methods.
- People with the "*appropriate security clearance and an assigned mission need",* as indicated by their security attributes and roles they are assigned to, are able to access data with corresponding attributes and roles. These assignments and entitlements are how *need to know* is expressed and implemented. No other 'need to know' check is performed – it is implicit in the request.

5.1 Key Concepts

5.1.1 Responsibility to Provide

Following 9/11, the clear need to improve data sharing led to a major paradigm shift in in the Intelligence Community. The Cold War stance of Need to Know (NTK) was modified in favor of the concept of Responsibility to Provide. ICPM 2007-200-2, "Preparing Intelligence to meet the Intelligence Community's Responsibility to Provide", and ICPM 2007-500-3 "Intelligence Information Sharing" directed the shift from data enclaves to data sharing among all intelligence elements, rescinding some directives that had prevented sharing in the past. ICD 501, "Discovery and Dissemination or Retrieval of Information Within the Intelligence Community", articulates the intent of the DNI:

"Responsibility to Provide.

a. IC elements shall fulfill their "responsibility to provide" by making all intelligence and intelligence-related information (hereinafter referred to as "information") that IC elements are authorized to acquire, collect, hold, or obtain (hereinafter referred to as "information collected") or analysis an IC element is authorized to produce discoverable by automated means by "authorized IC personnel," in accordance with Section D, unless otherwise exempt in accordance with Intelligence Community Policy Guidance (ICPG) 501.1, Exemption of Information from Discovery. Authorized IC personnel are individuals identified by their element head and who have an appropriate security clearance and an assigned mission need for information collected or analysis produced. "Discovery," as defined in Appendix A, is the act of obtaining knowledge of the existence, but not necessarily the content, of information collected or analysis produced by any IC element.
b. "Stewards," as defined in Appendix A, shall fulfill their "responsibility to provide" by making all information collected and analysis produced by an IC element ***available for discovery by automated means by authorized IC personnel*** *[emphasis added], unless otherwise determined by the DNI; by making as much information as possible available for automated retrieval upon discovery; and by* ***presuming that authorized IC personnel who request information discovered possess a "need to know****," in accordance with Section F."* – ICD 501

The Intelligence Community is directed to presume, in the absence of contrary indicators, that anyone authorized for access has a need to know. Marking all intelligence data/products with the proper security markings per DNI standards, such as the Intelligence Community Information Security Marking (IC ISM) metadata is one prerequisite. Others include maintaining entitlements categories and access roles associated with authorized personnel, and policy/rule-based automated enforcement mechanisms.

While not normally a Mission Data concern, we note that Personally Identifiable Information (PII) and Personal Health Information (PHI) is NOT covered by *Responsibility to Provide*. Specific, explicit and demonstrable *need to know* applies without exception.[49]

5.1.2 Authorized Data Access, rather than System Access

The Intelligence Community is directed to provide a means of automated discovery and retrieval for authorized personnel, by data content and data service without necessarily resorting to the legacy "owning" application. To state it clearly, access needs to be controlled and granted at the data level, not at the application level, to make Data-as-a-Service work. Individual systems can no longer be the sole gatekeepers to data access. All authorized people and entities must be

[49] DOD Directive 54O0.11, DOD Privacy Program.

able to get access to the data without setting up an account with a specific individual system or navigating through one owning application. Systems become the consumers of data instead of the owners of data.

5.1.3 Data Entitlements

Entitlements are rights and permissions that allow an entity privileges with data. ***Entitlements management*** is the set of procedures and technologies used to grant and revoke access rights and privileges to entities in support of authorization determination requirements.

Specific Entitlements control action permissions, e.g. an Entitlement might allow one to GET a dataset. Entitlements are used by policy-based rules (e.g. Policy Decision Points (PDPs)) to execute data access and provisioning decisions based on entity attributes and identifiers. Within a policy context, this represents the combination of

- privilege,
- entity (person entity (PE), or non-person entity (NPE) e.g. system) assigned an entitlement,
- applicable data, and metadata
- conditions (environment, time range, geographic range, etc.).

All of these are needed to determine accessibility, and the nature of that access. The other needed ingredient is the set of rules and methods that procedurally implement policy.

5.1.4 Data Privileges

When viewed from a Data viewpoint, there are a limited number of things a person can do with Data. These fall into three broad categories of Privileges: READ, MANAGE and ADMINISTER. The focus of this guidance is on READ and MANAGE.

- **READ** is when the entity has access to the data but is not able to change the data in the repository. The two specific access privileges for READ are:
    - LIST: This allows for a List/view of the data online. It does not allow for download. This is often equated to ICD 501 Discovery.
    - GET: This allows for the download of a copy of the data. This is often equated to ICD 501 Dissemination.
- **MANAGE** is the ability to change the data in some way. Some groups allow for Analysts to have some or all of the MANAGE privileges, others allocate some, or all, of these privileges to Administrators. The specific access entitlements for MANAGE are:
    - INSERT/PUT: The ability to “PUT” a new file in an S3 bucket or to “INSERT” a new record/document in a database.
    - APPEND: The ability to APPEND new information to an existing file/record/document without changing existing information. E.g. Doctors append new information to a medical record.
    - UPDATE: The ability to change information in an existing file/record/document.
    - DELETE: The ability to DELETE and existing file/record/document.

- **ADMINISTER**. The list of things an Administrator can do is far longer and is often more specific to the actual storage solution. However, some generic examples are the ability to backup and restore data.

5.2 Legacy Data Access

5.2.1 Legacy Activities

Current legacy activities act as the gatekeeper for their own data; the only way to get to the data is via the activity application, which one must have a login for. Some legacy activities validate the Identity of Users accessing the application with GeoAxIS, the NGA Enterprise Identity, Authentication and Authorization (IAA) Service Provider. Very few activities do actual authorization inside of their application, with most allowing complete READ access to everything in their system, if one has a login, and write access based on application roles. As such, most of the policy enforcement done by the application is really up front when setting up the user accounts: they validate that the user is allowed to see the data before granting an account.

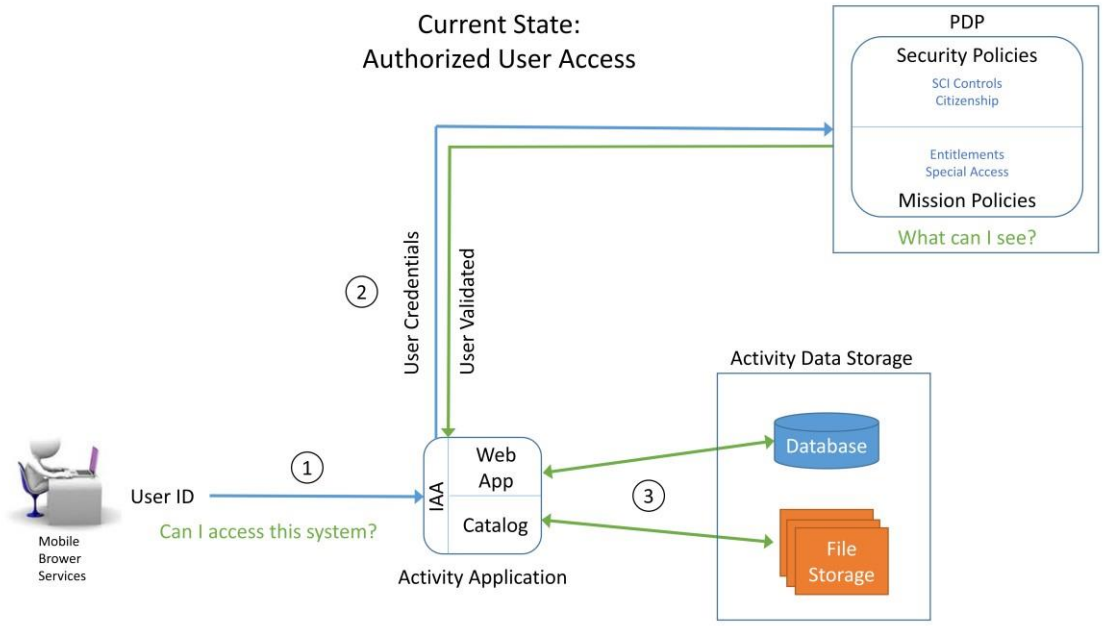


Figure 5-1: Legacy Data Access

Demonstrating the legacy data access, in Figure 5-1:

1. A user logs into the Activity Application with his User ID.
2. The IAA portion of the Activity sends that ID off to the Policy Decision Point (PDP) that validates whether he is an authorized user.
3. Once validated, he has access, via the application, to the database and file storage

that activity might control.

5.2.2 Legacy Network Access

One of the Data Access methods currently practiced at NGA is “if you have access to the network, you have access to the data”. This is also often referred to as Lowest Common Denominator (LCD). This was done in part because the data was not sufficiently marked to check by attribute. This practice also led to the setup of redundant sites and storage locations where NGA would duplicate subsets of data that specific mission partners were allowed to have and place it on their specific site because the mission partners could not be allowed access to the main network without exposing data they were not entitled to. The practice of duplication and subsets no longer is considered an appropriate solution. Going forward all data moving to the cloud will be conditioned with the appropriate metadata as specified in the metadata portion of the guidance. Data will be stored once and accessed as appropriate in accordance with the Data Access Vision.

5.3 Automated Data Access Vision

Data are tagged with Security and Access Metadata Attributes (including but not necessarily only ‘Classification and Control Markings’) specifying restrictions. On-line identities, for people (PE) or systems (NPEs), are tagged with authorization attributes, such as in the federated Authoritative Attribute Stores (AAS). Any additional access controls by role membership are also checked. The Enterprise PDP compares the data security attributes against the Entities’ authorization attributes and automatically allow or deny access to the Data.

The DNI concept of automated access and discovery with the appropriate clearance and assigned mission is served by two basic use cases: 1) Access by authorization attributes; 2) Access by role.

5.3.1 Access by Authorization Attributes

For an example, the Maritime Tactical Ocean Data 4 (TOD4) product is tagged as CONFIDENTIAL//NOFORN. No other special access or dissemination restrictions apply to the data set, so no role checks are necessary. Mary is a US Citizen with a Secret Clearance. Figure 5-2 illustrates how her attributes align. She will be granted access to LIST or GET TOD4.

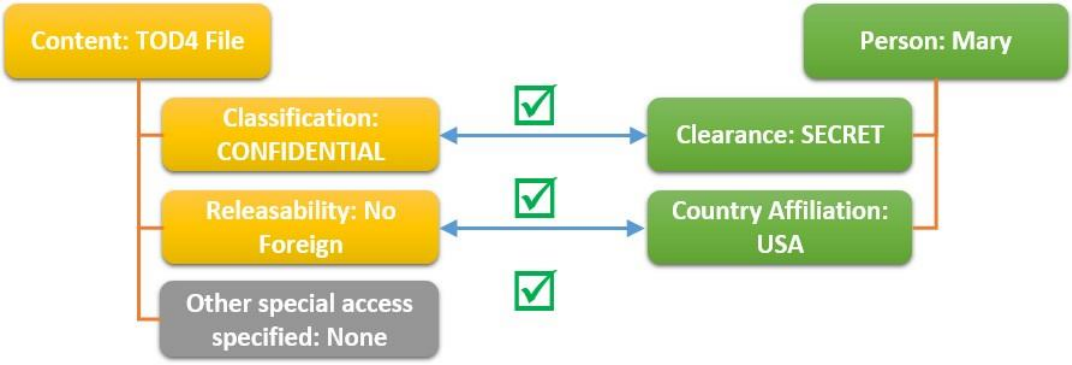


Figure 5-2: Security Matching Attribute: Mary

Bob is a liaison officer from the UK. He has a Top Secret Clearance. Bob will not be granted access to GET or LIST TOD4, as shown in Figure 5-3. If the TOD had been releasable to FVEY, Bob would have gotten the data.

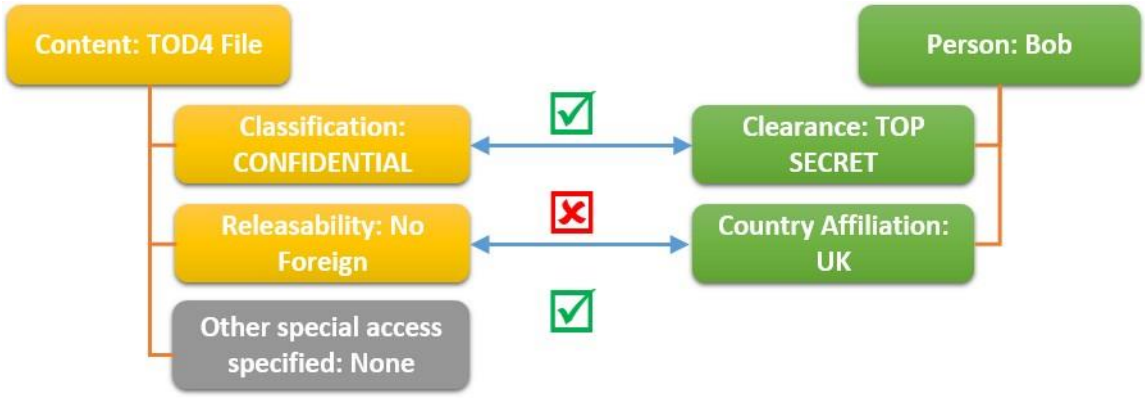


Figure 5-3: Security Matching Attribute: Bob

This type of access control is usually called Attribute Based Access Control (ABAC), where one's specific attributes allow access to the data.

5.3.2 Access by Role

Entitlements for restricted datasets are usually handled by specifying a "Group" that has access to the dataset, then confirming that users are group members. These groups are called roles in the Information Technology world. Roles usually are used for MANAGE access where there is a smaller set of users who can be provisioned into the group on an individual basis. They can also be used for READ access if there are special restrictions in place that cannot be covered by the authorization attributes.

This role paradigm serves no matter what the groups are based on; Proper Use Memorandum (PUM) controls, or restrictions based on intellectual property, international regulations or some other agreement binding on NGA.

The Entitlements Groups concept has four parts: The roles, the privileges, the data (e.g. Content IDs), and the entities associated with the role. With these four elements (illustrated in Figure 5-4), and a corresponding policy and rules set, any entitlements group based access can be automated.

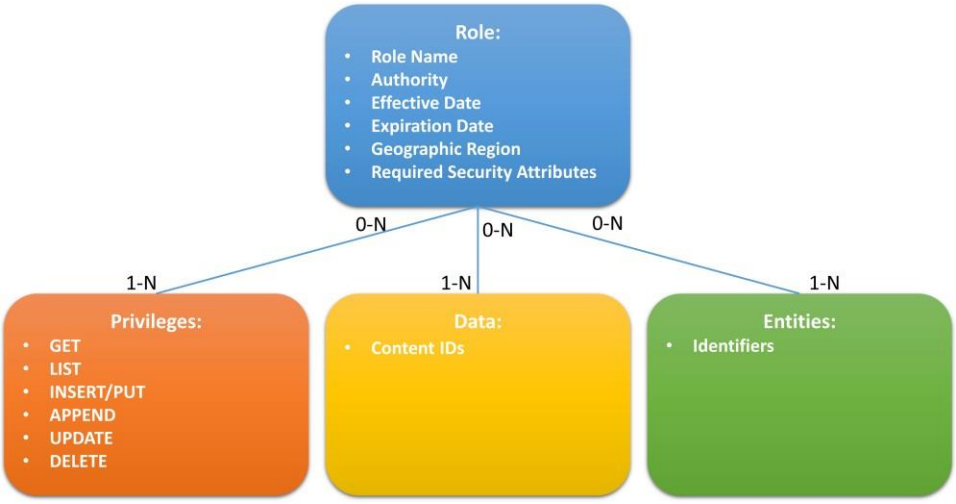


Figure 5-4: Entitlement Groups Concept

Data Custodians and Stewards will use Entitlement Management Services to create the roles, and define the privileges, data and entities that are associated to the roles. Changes might take minutes and would apply to any service or system using that data. In contrast, today the Activity's system team is typically asked to implement access changes, and without automation the changes can take days or weeks.

The following examples illustrate Entitlements Groups in two different use cases:

1. Statutory Restrictions
2. Proper Use Memorandum (PUM)

Because of international rules and regulations governing Aeronautical Safety of Navigation, only Aeronautical Analysts are allowed to access the Aeronautical production database and manage the data. Figure 5-5 shows how this group might be set up.

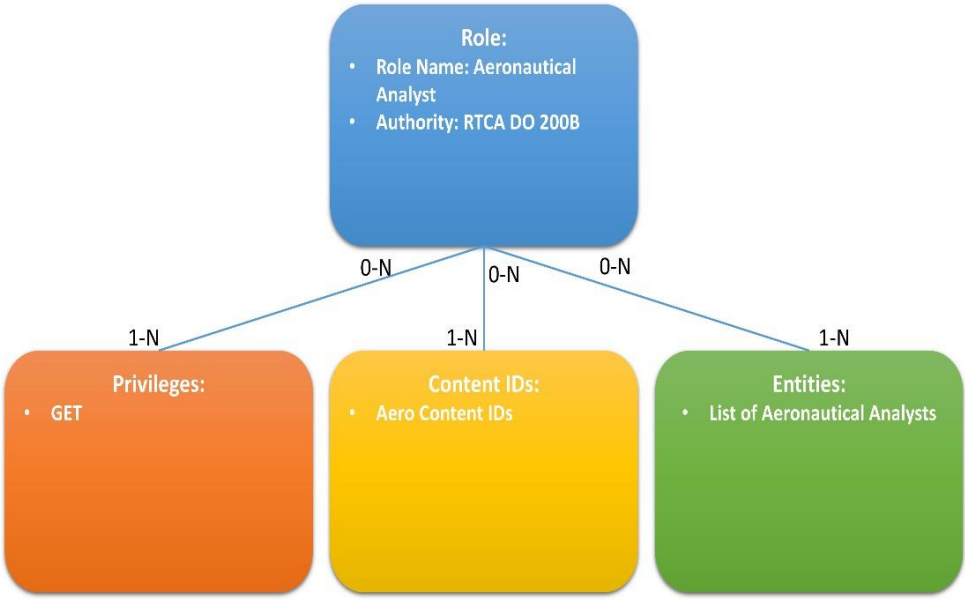


Figure 5-5: Aeronautical Analyst Entitlement Group Example

Figure 5-6: Cases like Hurricane Katrina, where a PUM was needed to handle domestic imagery, are also handled by this structure:

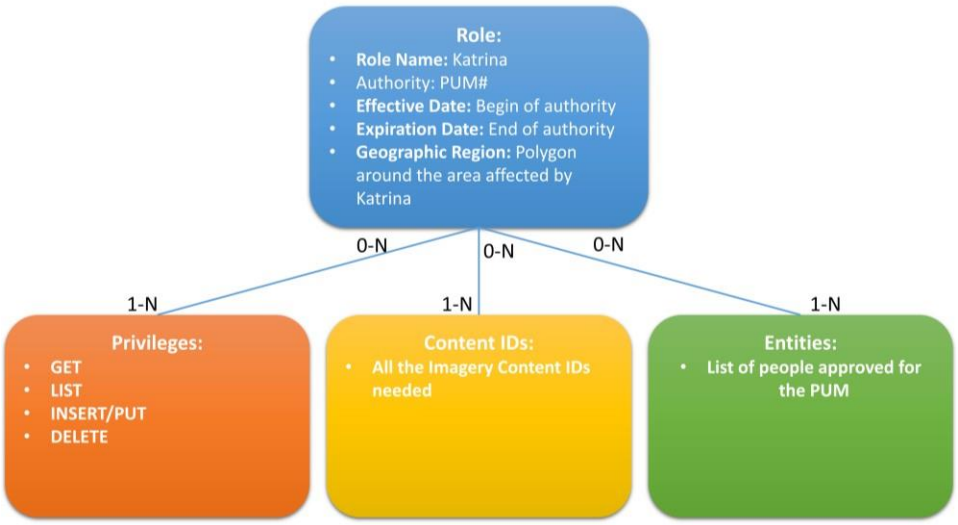


Figure 5-6: PUM Entitlement Group Example

No matter the reason for needing a group, a role can be defined, and privileges, data and entities assigned to it. This model can replace the custom authorization/role capabilities that

were traditionally custom-created for each legacy system. With this model, NGA can create an Enterprise Role Based Access Control (RBAC) capability that can be used by all systems.

5.3.3 Current State of Automated Data Access

GEOAxIS provides the Enterprise PDP capability. This PDP can perform the comparison of Person attributes to the Data attributes for authorization. GEOAxIS provides a role mechanism to the Enterprise that keeps the association of individuals and makes that available to applications. However, a full list of roles needed has not been determined, so it is unknown if all roles are currently defined in existing systems that perform authentication and authorization.

There is a now a Data Inventory where all Content IDs for NGA Data are defined, but the Content IDs are not yet associated with the roles. The DMWG has surveyed the Data Custodians to get an initial list of Data Entitlements for READ and MANAGE data privileges against the Content IDs.

Data is being migrated to the cloud, but the majority of it has not yet been conditioned.

Some parts are there, other parts are in the process of being built, but the entire architecture needed to achieve automated data access is not yet in place.

5.4 Roadmap to the Data Access Vision

The path forward has two distinct branches: File data, and databased data. It is the intention of the CDO to store File data in S3. So the two branches will be the S3 Data Access Roadmap and the Database Data Access Roadmap.

5.4.1 S3 Data Access Roadmap

Vision. As detailed in the Metadata portion of the Guidance, it is the intent of the CDO to stand up an Enterprise Metadata Catalogue that would have a record of each file stored in one of the S3 Buckets in the OpenDataStore. These records would include the Security Metadata both on the record itself, and on the Data in question. The Record Security Metadata would determine which results a person could see returned in a Metadata Catalog Query (LIST) while the Data security metadata would determine what data the user could download (GET).

The S3 future data access use case is demonstrated in figure 5-7.

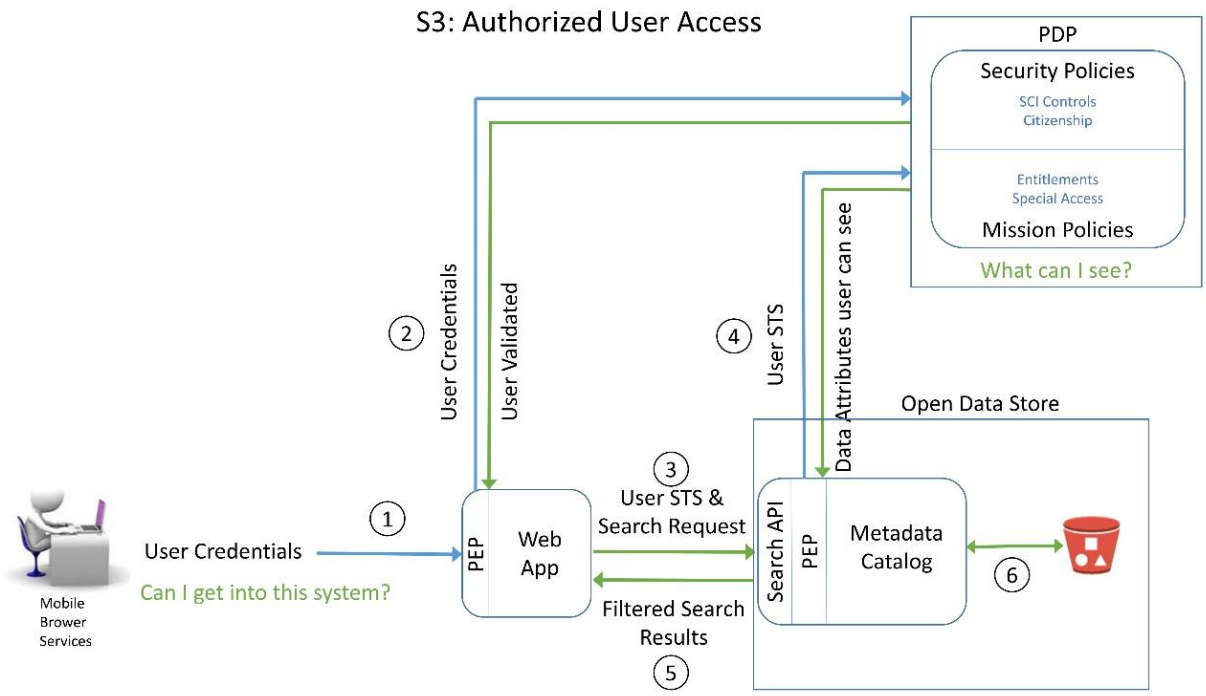


Figure 5-7: S3 Future Data Access

1. A user would submit his or her user credentials (PKI cert) to the Activity Application to access the application.
2. The application would Authenticate the user with the PDP. At this point, it still looks very like the legacy use case. However, along with the validation of the user, a Security Token Service (STS) token for that user is returned. That token is stored by the Activity Application for the session and is how the identity of the validated user is passed to the Data Services.
3. The user initiates a Search Request on the Metadata Catalog in the OpenDataStore. The Web Application passes his or her STS Token and the Search Request to the Search API.
4. The Search API uses the PEP to pass the user token to the PDP to determine what types of data the user is allowed to access. The PDP returns the policy constraints to the PEP.
5. The PEP applies filters to the Search Request such that Data the user cannot access is not even returned in the results. The Filtered results are returned to the Web Application and to the user
6. The user selects the data they want to access from the results list and executes a GET. This passes back through all the layers with the Metadata Catalog PEP, PDP etc. to ensure the user is only getting what they are allowed to get (making it so an ineligible user who has acquired a link cannot get the data) – and the files are disseminated to the user.

Current State. The current state of S3 Authorized User access is demonstrated in Figure 5-8.

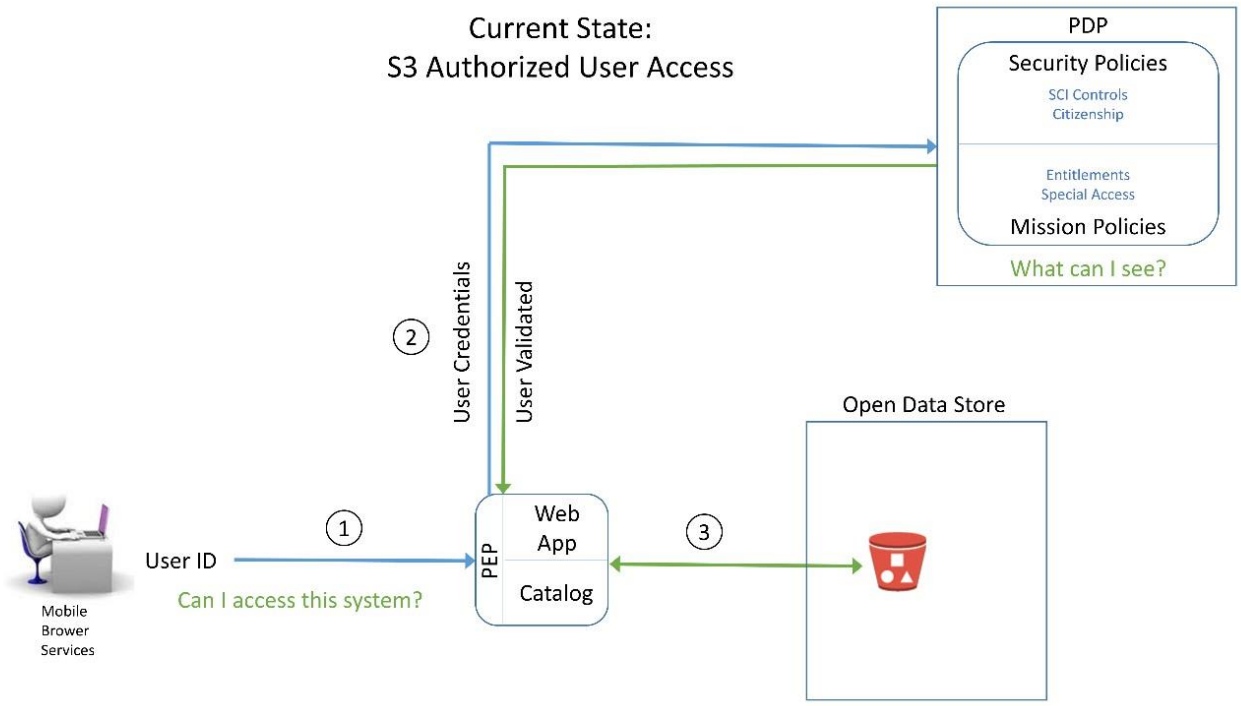


Figure 5-8: Current State of S3 Data Access

1. A user would submit his user credentials (PKI cert) to the Activity Application to access the application.
2. The application would Authenticate the user with the PDP.
3. The Web Application has full access to S3 Buckets and Content IDs it has been granted access to. There is no STS token being passed. There is no enterprise method for checking user attributes against data attributes.

GEOAxIS provides the Enterprise PDP capability. The Metadata Catalog and associated PEP are in the process of being built, but as of the writing of this document, not yet complete and exposed to the Enterprise.

This means that Activities cannot use the OpenDataStore Search API, PEP and Metadata Catalog. This necessitates allowing Activities Trusted Access directly to the S3 buckets and virtual folders to READ and/or MANAGE the data.

It is then up to those Activities with Trusted Access (hereafter referenced as Trusted Activities), to ensure that their users only have access to the appropriate data. In other words, they would operate much as they do now, with the exception that their data is stored in the

OpenDataStore.

Until such time that the OpenDataStore Search API, PEP and Metadata catalog are sufficiently matured and exposed to the enterprise, the only access to data will be via the Trusted Activities – which in most cases will be the Legacy systems.

Going Forward. The OpenDataStore Search API, PEP and Metadata catalog will be matured, with capabilities released in phases as they are available. A Phase I solution to the Vision, for instance, might have a PEP/PDP combination that only has the ability to compare person attributes for Clearance, Country affiliation and SCI controls to grant basic GET and LIST entitlements. This would restrict the OpenDataStore services to only serving data out, via the Enterprise Services, that could be released based on those attributes.

A Phase II solution will enable a PEP/PDP combination that could handle role based entitlements. This would not only expand the data with READ privileges but would enable the PDP and PEP to broker MANAGE privileges as well.

As the Enterprise solutions in the OpenDataStore are able to perform the brokering on both READ and MANAGE privileges, new Activities will be required to use the Enterprise services. Legacy activities that will persist long term will also be required to shift over to the use of the Enterprise Services instead of maintaining their own.

5.4.2 Database Data Access Roadmap

Vision. The intent of the CDO is to support Fine Grained Access control of Data within Databases. To do this, security metadata, as defined by the IC ISM standards, must be present in the database at the very least at a Row/Object/Document level, and, ideally, at an attribute/key/value pair level.

The IC ISM standard has been incorporated into the NMF, and into the latest version of the NAS. So, databases whose schema is IC ISM compliant should be able to implement/use Enterprise PEP/PDP services for fine grained data access control on their database. The database future data access use case is demonstrated in figure 5-9.

1. A user would submit her User credentials (PKI cert) to the Activity Application to access the application.
2. The application would Authenticate the user with the PDP. At this point, it still looks very like the legacy use case. However, along with the Validation of the user, an STS token for that user is returned. That token is stored by the Activity Application for the session and is how the identity of the validated user is passed to the Data Services.

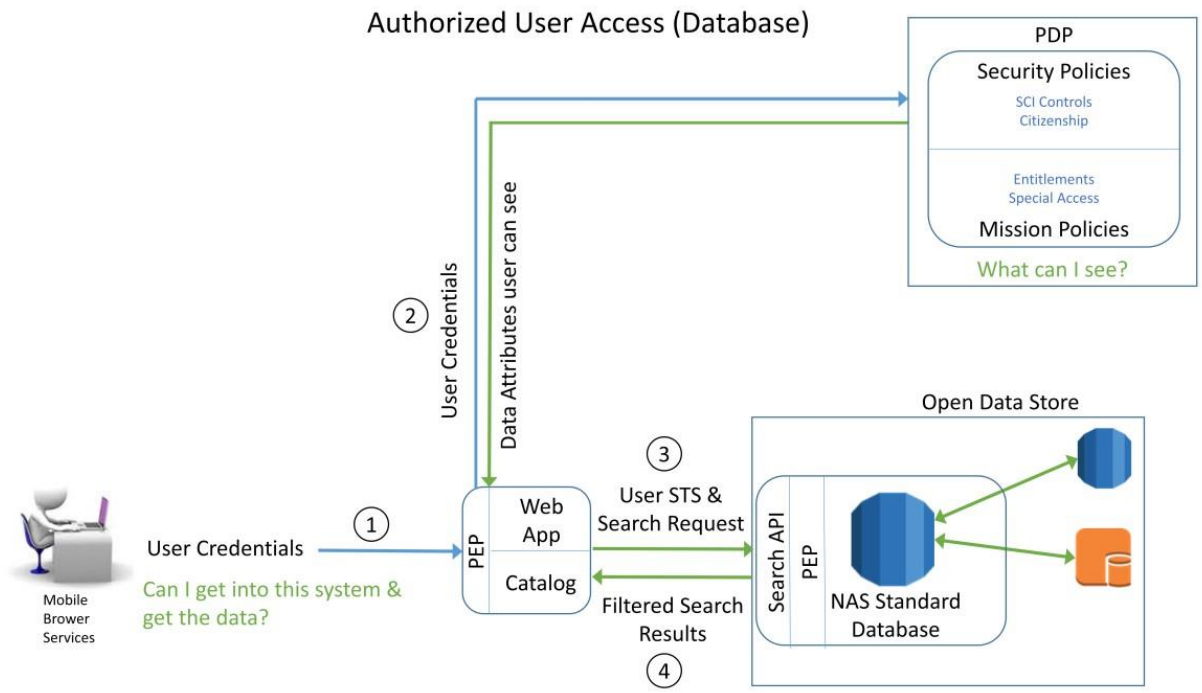


Figure 5-9: Database Future Access

3. The user initiates a Search Request on the database in the OpenDataStore, using the Web Application. The Web Application passes her STS Token and the Search Request to the Search API.
4. The PEP applies filters to the Search Request such that Data the user cannot access is not even returned in the results. The Filtered results are retuned to the Web Application and to the user

Note that the STS token is used differently in this example than in the S3 example. In the S3 example, the STS token was just used to pass the authenticated user identity, and a second query to the PDP was used to apply the policy constraints. In this example, the first query to the PDP is not only getting the validation of the user, the data attributes the use case see – such that a second query is not needed to create the filter. The NRO, DNI and NGA are still working on their final answer to bulk authorization and which method will be used will be dependent on those decisions. Future guidance will contain any refinements/updates based on those decisions.

Current State. There are a large number of legacy production and dissemination databases. While some of the legacy activities use GEOAxIS for authentication, almost none of the databases do any sort of authentication. Almost none of them use the PDP for authorization. Most of them have their own custom version of Data Access control. Most of them are also tightly coupled to their respective activities, and any change in schema to accommodate the IC

ISM would require enormous transformation to the Activity.

Currently, the only way to access the legacy databases, whether in the Data Center or in the OpenDataStore, is via the Legacy Activity that MANAGEs that data.

Going Forward. Realizing that transforming all of the legacy databases and their associated legacy application would be “a bridge too far”, the CDO is working to set up a NAS compliant database for NGA content that has previously been mapped to the NAS. This would work as a dissemination database, with the output of the various legacy databases being propagated to the new enterprise NAS based database. This could either be a physical database into which the production data is loaded, or a data virtualization capability that performs on the fly transformations to the NAS standard. This would enable both automated enterprise data access with fine grained control, as well as enhanced discovery using the NSG standard definitions of entities and attribute found in the NAS.

For content that has not previously been mapped to the NAS, but would be appropriate to add to the NAS, the CDO office will work with the Data Custodian and the NSG Standards office to get the content incorporated.

For content that is not appropriate for the NAS but would still like to take advantage of the automated, fine grained access control, the CDO office will work with the Data Custodian to get the IC ISM incorporated into their schema.

5.5 Impacts

5.5.1 Future Development

With the stated vision for Data Access and Handling, the obvious question is: “How it will impact future application development?” There will be two main effects on development:

- Applications will not have to build their own authentication and authorization and create their own logins and roles. Developers will instead be able to use enterprise authentication and authorization services.
- Applications will have to be able to propagate identity via STS tokens back to the data services to get the correct results. In the past, identity often ended at the front door of the applications, with all other actions taken by the application as an NPE.

5.5.2 Enterprise

The impacts at the enterprise level are even larger than those at the development level:

- Removing the need for individual systems to create their own log-ins means that a single sign-on enterprise would really be possible
- Removing the need for individual systems to implement their own entire authorization capability also paves the way for microservices instead of the monolithic legacy systems of the past

- Identity Propagation by all the applications and services involved in any sort of transaction would make it much easier to do real audit logging without having to do forensics back through all the various applications and services to figure out who really initiated it
- Data Access based on attributes and roles, with data properly metadata tagged, removes the need to have separate networks and storage for different groups/people with different access levels, our foreign partners in particular. With information automatically filtered by the services to what a person is allowed to see, redundant networks and storage for the different group are no longer needed

APPENDIX G-A: DEFINITIONS

UNCLASSIFIED	
Term	***Definition***
Activity	Per the CAMG “Activity” replaces the words application, system, entity, capability and program.
Activity Data	This is the technical data needed to make an activity/service run. This excludes mission content. This includes code, configuration files, logs, etc.
Analytic Registry and Repository/Catalog	The analytic registry will store artifacts software logic (such as XML Schema Definition documents, Web Service Description Language documents, and Service Level Agreements) related to analytic services and web enabled application interfaces (i.e., widgets and apps). Services and other software applications will use this repository at run time to search for specific analytic services and to retrieve service endpoints for invoking those services. Content producers will add and modify entries in the service registry as part of the process for service-enabling their content. An analytic catalog or repository containing human-readable descriptive information (metadata) about analytic services will serve as the user-facing repository that content producers, analysts, data scientists, and others use to discover information on analytic services. The analytic repository or catalog is conceptually distinct from the analytic registry but may be physically integrated with the registry implementation. The Analytic Registry can be part of the Service Registry and Repository/Catalog.
Analytical Data	This is the ephemeral working data/products that Analysts are analyzing on their desktops on in an Analytical Tool/Service. It is not considered Mission Data until it is finalized/published to the gold repository and/or the customer. The published product created from the results of Analytical Data are an example of Mission Data.
Archive	Stored infrequently used data (e.g., AWS Glacier data objects or set of objects identified by an AWS Archive ID; archives are stored in an AWS Glacier Vault.)
Big Data	Refers to massive datasets and combinations of datasets with size and complexity beyond the ability of traditional software and tools to capture, store, manage, and analyze. As distinct from “Large Data”, which refers to individual files, each of which is very large.
Conditioning (data)	Conditioning is the research and addition of metadata to the catalog to support enterprise discovery.
Content	Data, products, services, and knowledge that are discoverable and accessible. In AWS, any data in any format.
Content Collection Catalog	The Content Collection Catalog will provide a directory of the types of content available within the NGA enterprise. It will contain metadata describing each type of content, including its form, functions, access restrictions, suitability for use, inventory status, and associated points of contact. This catalog will serve as a tool enabling users to discover the kinds of content available to them. It will also be a means for enabling effective content governance, consistent web navigation of content, and compliance with content standards.

Term	*Definition*
Corporate Data	Data used at the enterprise level that enables the business of NGA but is not directly part of the mission. This would include PeopleSoft Data, GeoAxis Data, and other Enterprise Needs/Workflow/Process tools. This varies from the Conceptual Data model definition of corporate data in that activity data is excluded.
Dataset	A collection of data.
Data Lake	A large storage repository and processing engine that provides "massive storage for any kind of data, enormous processing power and the ability to handle virtually limitless concurrent tasks or jobs".
Master Data Catalog	A subset of the Object Instance Catalog, it is the single source of basic business data used across all systems, applications and processes for the enterprise.
Metadata	Data about data; graphical or textual information about the content, quality, condition, origins, and characteristics of data.
Metadata Catalog	The Metadata Catalog is a human readable collection of metadata for file-based data.
Mission Data	Data used in performance of the NGA Mission, which would be considered “Gold Copy” or Record data. This would include source data (*host nation publications, imagery, commercially purchased datasets etc.*), the actual production data stores (*ex: Aeronautical Migration System (AMS) Databases Aeronautical Obstruction Environment (AOE) and Aeronautical Digital Data Environment (ADDE), Topographic Features Data Management (TFDM) Topographic Data Store (TDS)*) and data stores *(ex: Web Digital Vertical Obstruction File (WebDVOF) Database) / products (Digital Nautical Chart (DNC), Intel Reports, Geodesy Models, Navigation Planning (NAVPLAN) Charts, Controlled Imagery)/publications (Flight Information Publication (FLIP), American Practical Navigator, Fleet Guides etc.)* that NGA disseminates. This is “the content”.
Object	Binary Large Object (BLOB), file or other data set, identified by a key. Also, representation of physical or conceptual objects and their activities.
Object Catalog	Contains entries describing discrete instances of objects (for both Mission and Corporate data). The object catalog is a metadata catalog in which discrete instances of object data are described by a single record (row) in the catalog database. The Object Catalog is conceptually distinct from the Metadata Catalog (a component of NGA’s enterprise search capability architecture) but may be physically integrated with the implementation of the Enterprise Metadata Catalog. Each object catalog entry will contain a Universally Unique Identifier (UUID) for an object instance, descriptive metadata to enable discovery and search, IC mandated metadata relating to security classification and access control, and a machine resolvable link (such as URL (Uniform Resource Locator)) to enable access to the object.
Organizational Data	A subset of Corporate data – files and data organizations generally put in their shared organization drives now (a migration–specific category). This is data needed for the business process of individual organizations. This would include things like International Standards Organization (ISO)

Term	Definition
	processes, Org Charts, briefings… the types of things organizations generally put in their shared organization drives or SharePoint.
Product	Data that is a packaged result of NGA effort, as opposed to raw data from outside sources.
Scalability	Data transaction or storage amount increases or decreases with performance neutrality.
Semantics Catalog (Controlled Vocabulary (CV) Registry)	A directory of pre-defined vocabulary schemas including taxonomies, synonym lists (thesauri), approved keyword lists, and other knowledge organization schemas (ontologies). The controlled vocabularies will be searchable and accessible for use in content preparation activities (such as metadata tagging), providing user selections in search query construction, and enabling semantic search capabilities. One of the principal taxonomies in the current NGA enterprise is the NSG content taxonomy that defines hierarchical categories describing the primary form and mission of each type of NGA managed content. The NSG content taxonomy will be the basis for identifying and describing entries in the Content Collection registry.
Service Registry and Repository/Catalog	The service registry will store artifacts (such as XML Schema Definition documents, Web Service Description Language documents, and Service Level Agreements) related to enterprise web services and web-enabled application interfaces (i.e., widgets and apps). Services and other software applications will use this repository at run time to search for specific web services and to retrieve service endpoints for invoking those services. Content producers will add and modify entries in the service registry as part of the process for service-enabling their content. A service catalog or repository containing human-readable descriptive information (metadata) about web services will serve as the user-facing repository that content producers, system developers, and other users can use to discover information on enterprise web services. The service repository or catalog is conceptually distinct from the service registry but may be physically integrated with the service registry implementation.

APPENDIX G-B: ACRONYMS

UNCLASSIFIED	
Term	***Definition***
A&A	Assessment and Authorization (access permission determination)
AAS	Authoritative Attribute Stores
ABAC	Attribute Based Access Control
ADDE	Aeronautical Digital Data Environment
AMI	Amazon Machine Image
AMS	Aeronautical Migration System
AOE	Aeronautical Obstruction Environment
AR	Architecture Repository
ARH	Access Rights and Handling
ASP	Application Service Provider
ATO	Authority to Operate
AWS	Amazon Web Services
BLOB	Binary Large Object
C2S	Commercial Cloud Services – a Cloud service provided by Amazon data services network
CAMG	Cloud Adoption Management Group
CDO	Chief Data Officer
COTS	Commercial off-the-shelf
CRQ	Change Request
DAFIF	Digital Aeronautical Flight Information File
DAR	Data at Rest
DIT	Data in Transit
DNC	Digital Nautical Chart

Term	Definition
DNI	Director of National Intelligence
DSP	Data Service Provider
EBS	Elastic Block Storage (AWS storage volume Service)
EC2	Elastic Compute Cloud (AWS Virtual Machine Service)
EDH	Enterprise Data Header
FLIP	Flight Information Publication
FOC	Final Operational Capability
GUIDE	Global Unique IDentifier for Everything
I&A	Information and Assurance
IAA	Identity, Authentication and Authorization
IAM	Amazon Identity and Access Management
IdAM	Identity Access Management
IC	Intelligence Community
IC ISM	Intelligence Community Information Security Marking
IC ITE	Intelligence Community Information Technology Enterprise
ICD	Intelligence Community Directive
IC-GovCloud	Intelligence Community Government Cloud (a Cloud service)
IOC	Initial Operating Capability
ISM	Information Security Marking
ISO	International Standards Organization
ISP	Infrastructure Service Provider
LCD	Lowest Common Denominator
MLS	Multi-Level Security

Term	Definition
NARA	National Archives and Records Administration
NAVPLAN	Navigation Planning
NCL	NSG Consolidated Library
NGA	National Geospatial-Intelligence Agency
NITF	National Imagery Transmission Format
NMF	NSG Metadata Foundation
NOSQL	Not Only Structured Query Language
NPE	Non-Person Entities (e.g. automated systems or organizations)
NSG	National System for Geospatial Intelligence
NTK	Need to Know
OCIO	Office of Chief Information Officer
ODNI	Office of the Director of National Intelligence
OS	Operating System
PDP	Policy Decision Point
PE	Person Entities
PEP	Policy Enforcement Point
PII	Personal Identifying Information
PHI	Personal Health Information
PMO	Program Management Office
POC	Point of contact
POM	Program Objective Memorandum
PoR	Program of Record
PUM	Proper Use Memorandum

Term	*Definition*
RBAC	Role-Based Access Control
RDS	Relational Database Services (AWS Managed Service Category)
S3	Simple Storage Service (AWS object storage service)
SAP	Special Access Program
SFA	Foundation GEOINT Aeronautical Navigation Office
SSH	Secure Shell
STS	Security Token Service
TDF	Trusted Data Format
TDO	Trusted Data Objects
TDS	Topographic Data Store
TEM	Technical Exchange Meeting
TFDM	Topographic Features Data Management
TMS	Target Management System
U-AWS	Unclassified Commercial Cloud (An Amazon Web Services offering)
UC	Unclassified Cloud
URL	Uniform Resource Locators
UUID	Universally Unique Identifier
WebDVOF	Web Digital Vertical Obstruction File
WFS-T	Transactional Web Feature Service
XML	Extensible Markup Language

APPENDIX G-C: REFERENCES

Intelligence Community Technical Specification IC Enterprise Attribute Exchange between IC Attribute Services Unified Identity Attribute Set, 13 August 2015

Intelligence Community Technical Specification XML Data Encoding Specification for Access Rights and Handling, 6 September 2013

Intelligence Community Technical Specification, XML Data Encoding Specification for Trusted Data Format, 17 July 2012

Intelligence Community Technical Specification, XML Data Encoding Specification for Enterprise Data Header, 13 August 2015

Intelligence Community Technical Specification, XML Data Encoding Specification for Information Security Markings, 13 August 2015

Intelligence Community Technical Specification XML CVE Encoding Specification for ISM Country Codes and Tetragraphs, 2015-NOV and Annexes

Intelligence Community Technical Specification, XML Data Encoding Specification for Need to Know Metadata, Version 13 August 2015

Intelligence Community Directive 501 "Discovery and Dissemination or Retrieval of Information within the IC"

Intelligence Community Standard 500-21 Tagging of Intelligence & Intelligence Related Info, 28 January 2011

Intelligence Community Standard 500-30 Enterprise Authorization Attributes, 24 April 2014 NCD 8000-003 Encryption of Data at Rest

Intelligence Community Policy Guide 500.2 Attribute Based Authorization and Access Management, 23 November 2010

Intelligence Community Policy Guide 501.1 Exemption of Information from Discovery, 26May2009
Intelligence Community Policy Guide 502 Attribute-Based Authorization and Access Management IC Cloud Baseline 1.0 (CB1)

IC Cloud Baseline 2.0 (CB2)

IC-TDF Resources and Library, http://intellipedia.intelink.ic.gov/wiki/TDF “Pentaho, Hadoop and Data Lakes”, James Dixon’s Blog

Intelligence Community Technical Specification, Abstract Data Definition for Electronic Records Management, Version 2014-DEC

NGA Standardization Document National System for Geospatial Intelligence Metadata Foundation (NMF) – Part 1: Core (2014-09-23) Version 2.2

NGA Standardization Document National System for Geospatial Intelligence Metadata Foundation (NMF) – Part 4: Records Management Metadata (2015-04-03) Version 2.0

NGA Data Management Guidance, 016NGA Unified Data Strategy (UDS), 2015

APPENDIX G-D: (RESERVED)

APPENDIX G-E: NMF MANDATORY FIELDS

G-E.1 NGA NMFv3 Mandatory Fields (REVISED!)

The following fields are the minimum required fields specified by NMF version 3.0. They are listed in the order they were specified. These fields are designed to support the several data categories required for file based discovery in the cloud.

The NMF version 3.0 specification is found in the following location within the NGS Standards Registry: https://nsgreg.nga.mil/doc/view?i=4252

NMF metadata that is included in a TDF package is added to the portions of the xml documentation that are referred to as the “other or mission assertion” related elements.

UNCLASSFIED		
NMF 3.0 Required Fields		
Metadata Tag	***Description***	***Domain Guidance***
Metadata Point of Contact	The party or parties acting in a role of responsibility for a set of resource metadata.	The first instance of this element is to have the role of “creator”. Resource Metadata (Table 7) Metadata Contact – Populate using the Responsibility datatype (Table 46) with role (Table 3) of ‘pointOfContact’ and identifying the individual or organization responsible for the metadata record.
Metadata Date	The date(s), and optionally time(s), of an event involving a set of resource metadata.	The first instance of this element is to have the role of “creation”. Resource Metadata (Table 7) Resource Metadata Date – Populate using Date datatype (Table 50) with the date and DateType (Table 3) such as ‘creation’, ‘publication’, or ‘revision’ for when the metadata record was created, published, or revised.

UNCLASSFIED		
NMF 3.0 Required Fields		
Metadata Tag	*Description*	*Domain Guidance*
Metadata Standard Title	The name of the metadata standard which determines the structure and content of this set of resource metadata.	Resource Metadata (Table 7) Metadata Standard Citation – Populate using Citation datatype (Table 45) identifying the Cited Resource Title of the standard used for the metadata record. NSG Metadata Foundation (NMF), Version 3.0 10
Metadata Standard Edition	The version of the metadata standard which determines the structure and content of this set of resource metadata.	Resource Metadata (Table 7) Metadata Standard Citation – Populate using Identifier datatype (Table 54) identifying the code for the edition of the standard used for the metadata record.
Metadata Scope Code	A brief indicator of the type of resource for which metadata information is reported.	Metadata Scope (Table 8) Resource Scope – Populate using ScopeCode codelist (Table 3) to identify the type of resource the metadata applies to such as ‘dataset’, ‘series’, ‘attribute’, or ‘feature’.
Metadata Scope Name	A word or phrase that describes the type of resource for which information is reported.	Metadata Scope (Table 8) Resource Scope – Populate using Resource Scope Name identifying type of resource if Resource Scope is not ‘dataset’.
Metadata Classification	The classification level of the metadata, in accordance with the Intelligence Community (IC) Security Markings Manual.	Security Attributes Group (Table 33) Resource Classification – Populate with ResClassificationStrucText datatype (Table 33).
Metadata Classification System	The classification system of the metadata, in accordance with the Intelligence Community (IC) Security Markings Manual.	Security Attributes Group (Table 33) Resource Owner-Producer – Populate with ResOwnerProducerStrucText datatype (Table 33).
Resource Title	The name by which a cited resource is known.	Identification (Table 9) Resource Citation – Populate with using Cited Resource Title (Table 45).

UNCLASSFIED		
NMF 3.0 Required Fields		
Metadata Tag	***Description***	***Domain Guidance***
Resource Abstract	A brief statement or narrative summary of the resource.	Identification (Table 9) Resource Abstract – Populate with free text providing a short description of the resource.
Resource Point of Contact	The party(ies) acting in a role of responsibility for the resource.	The first instance of this element is to have the role of “originator”. Identification (Table 9) Resource Point of Contact – Populate using the Responsibility datatype (Table 46) with role (Table 3) of ‘pointOfContact’ and identifying the individual or organization responsible for the metadata record. NSG Metadata Foundation (NMF), Version 3.0 11
Resource Date	A reference date for a cited resource. The first instance of this element is to have the role of “creation”.	Identification (Table 9) Resource Citation – Populate using Date datatype (Table 50) with the date and DateType (Table 3) such as ‘creation’, ‘publication’, or ‘revision’ for when the metadata record was created, published, or revised.
Resource Identifier	A value uniquely identifying the resource within a namespace.	Identification (Table 9) Resource Citation –Populate using Identifier datatype (Table 54) identifying the code for the unique resource identifier.
Resource Geographic Location	The spatial extent of the resource. The spatial extent is a geographic identifier (for example: a country name), a bounding box (for example: the bounding latitudes and longitudes), or a bounding object (for example: a set of coordinate points).	Identification (Table 9) Resource Extent – Populate using Geographic Extent datatype (Table 39) to specify a Geographic Bounding Box, Geographic Description, or Geographic Bounding Object.

UNCLASSFIED		
NMF 3.0 Required Fields		
Metadata Tag	*Description*	*Domain Guidance*
Resource Language	Designation of the locale language.	Data Identification (Table 10) Text Locale – Populate using Language Locale (Table 55) LanguageCode codelist (Table 3) to identify language of resource.
Resource Character Set	Designation of the character set to be used to encode the textual value of the locale.	Data Identification (Table 10) Text Locale – Populate using Locale Character Encoding (Table 55) IANA Charset codelist (Table 3) to identify character set used in resource.
Resource Topic Category Code	A theme or topic keyword that represents a subject of the resource.	Identification (Table 9) Topic Category – Populate using MD_TopicCategoryCode enumeration (Table 4).
Resource Keywords	Information about keywords describing this resource.	Keywords (Table 12) Keywords – Populate with Keyword to identify content of the resource.
Resource Classification	The classification level of the resource, in accordance with the Intelligence Community (IC) Security Markings Manual.	Security Attributes Group (Table 33) Resource Classification - Populate with ResClassificationStrucText datatype (Table 33).
Resource Classification System	The classification system of the resource, in accordance with the Intelligence Community (IC) Security Markings Manual.	Security Attributes Group (Table 33) Resource Owner-Producer – Populate with ResOwnerProducerStrucText datatype (Table 33). NSG Metadata Foundation (NMF), Version 3.0 12
Resource Category	The particular category of a data resource within a defined taxonomy.	Resources within a category have similar information content and have been produced by similar processing methods. The default is a resource category type of "other". NMF Data Identification (Table 11) Data Identification – Populate with Resource Category using

UNCLASSFIED		
NMF 3.0 Required Fields		
Metadata Tag	*Description*	*Domain Guidance*
		code from ResourceCategoryCode codeList (Table 3).
Metadata Language	Designation of the locale language.	Obligation: Required when not defined by encoding. Data Identification (Table 10) Text Locale – Populate using Language Locale (Table 55) LanguageCode codelist (Table 3) to identify language of resource.
Metadata Character Set	Designation of the character set to be used to encode the textual value of the locale.	Data Identification (Table 10) Text Locale – Populate using Locale Character Encoding (Table 55) IANA Charset codelist (Table 3) to identify character set used in resource.
Parent Metadata Citation	A standardized reference to a set of metadata that is in a parent relationship to this set of resource metadata.	Obligation: Required if there is an upper scope Level. Identification (Table 9) Parent Metadata Citation – Populate using Citation datatype (Table 45) identifying the identifier of parent metadata.
Resource Temporal Extent	The time period covered by the resource	Obligation: Required when Resource Extent Description, or Geographic Extent, or Vertical Extent not documented. Temporal Extent (Table 43) Temporal Extent – Populate using Temporal Geometric Primitive (Table 60), such as Temporal Period or Temporal Instance.

UNCLASSFIED		
NMF 3.0 Required Fields		
Metadata Tag	*Description*	*Domain Guidance*
Resource Coordinate Reference System	Information about a spatial or temporal reference system used by representations in the resource.	Obligation: Required if the resource includes coordinates. Reference System Information (Table 37) Reference System Identifier – Populate with Identifier (Table 54) Code identifying the reference system used in the resource.

G-E.2 NGA Analysis and Source Mandatory Fields (REVISED!)

The NGA Source Organization provided feedback for the following fields that are deemed essential and necessary for file based discovery and these fields are provided as a requirement for essential metadata file based discovery in the cloud.

UNCLASSIFIED	
NGA Analysis and Source Mandatory Fields	
Metadata Tag	*Definition*
Abstract (Resource)	Brief narrative summary of the content of the resource(s)
Classification	Classification of material to be published
Classification System	Name of the classification system
Content (Resource) POC	Party (Person or Organization) responsible for the resource
Date (of Cited Source)	Date for the cited resource
Date Posted (or Published)	Date that the resource data was posted or Published
Dissemination Controls	One or more indicators identifying the expansion or limitation on the distribution of information
Geographic Location (Extent)	Location that the published material covers
Identifier (Resource)	Alphanumeric value identifying the resource

UNCLASSIFIED	
NGA Analysis and Source Mandatory Fields	
Metadata Tag	***Definition***
Keyword	Specified by a controlled-vocabulary code or by keywords.
Metadata Date Stamp	Date that the metadata was created
Metadata Language	Language used for documenting metadata
Metadata POC	Party (Person or Organization) responsible for the metadata information
Metadata Standard Name	Name of the metadata standard (including profile name) used
Metadata Standard Versions	Version (profile) of the metadata standards used
Releasability	Information explicitly marked for appropriate foreign disclosure or release
Resource Language	Language(s) used within the dataset
Review Date (Not used by A)	Date the material is to be reviewed for accuracy (one year after published date)
Resource Character Set	Full name of the character coding standard used for the dataset
Resource Originator POC	Party (Person or Organization) who created the resource
Resource Topic Category	Main theme(s) of the dataset
Temporal Extent	Information about the temporal extent of the resource
Title (Resource)	Name by which the cited resource is known
Online Resource	Information about on-line sources from which the resource can be obtained

G-E.3 NGA X Organization Mandatory Fields (REVISED!)

The NGA X Organization provided the following list of fields that are deemed essential and necessary for file based discovery. These fields required and essential metadata for file based discovery in the cloud.

UNCLASSIFIED	
NGA X Organization Mandatory Metadata	
Metadata Tag	***Definition***
Nominator Name	Indicates user who nominated the object
Nominator Email	Indicates email of nominator
Content URL	Provides reference location to object
Content Name	Indicates object name
Keywords	Metadata that describes object in one word
Contend Description	Informs potential user of data object's subject
Content Mission	Indicates object's mission association
Licensing Agreements/Restrictions	Indicates legal usage of object
Which security network I find this product on	Provides reference location to object by security network
Maintenance Cycle/Update Frequency	Indicates how often object is updated
Data Type	Indicates data type (file type)
Event or NGA Crisis Action Team	Indicates whether or not the data supports an Event or NGA Crisis Team
Content Owner Name	Indicates who can be questioned about the object
Organization/Office/Branch	Indicates the Org./Office/Branch that the Content Owner supports
Organization/Office/Branch Email	Indicates Organization/Office/Branch Email – Contact Information
Organization/Office/Branch Phone	Indicates Organization/Office/Branch Phone – Contact Information

APPENDIX G-F: CROSS REFERENCE NMF WITH EDH AND TDF

Placeholder: Cross Reference NMF with EDH and TDF.

UNCLASSFIED		
Cross Reference NMF with EDH and TDF		
NMF Metadata Tag	***EDH Mapping***	***TDF***
Resource Date	Create Date	Applies to Payload
Metadata Point of Contact	Responsible Entity	Applies to Mission Assertion
Metadata Date Stamp	Create Date	Applies to Mission Assertion
Metadata Security Classification	ARH/ISM/Classification	Applies to Handing Assertion
Metadata Security Classification System	ARH/ISM/Owner Producer	Applies to Handling Assertion
Resource Security Classification	ARH/ISM/Classification	Applies to Payload
Resource Security Classification System	ARH/ISM/Owner Producer	Applies to Payload
Resource Identifier	Identifier	Applies to Payload
Resource Originator	Responsible Entity	Applies to Payload
Resource Point Of Contact	Responsible Entity	Applies to Payload

APPENDIX G-G: IC MANDATORY FIELDS (*NEW*!)

G-G.1 Electronic Records Management (ERM) (REVISED!)

Electronic Records Management (ERM) is an IC mandatory standard and is required to provide the means to audit, track, and manage disposition information.

The ERM specification is found at the following location within the IC Technical Specifications Library:

https://intelshare.intelink.ic.gov/sites/odni/cio/me/techspecs/Documents/erm/default.aspx

ERM has a dependency with the standards show in the following table:

UNCLASSFIED			
ERM Dependent Standards			
Abbreviation	***Category***	***ID***	***Title***
TDF	Packaging/Transport	IC-TDF.XML.V2014-DEC	XML Data Encoding Specification for Enterprise Data Header, Version 2015-AUG
ISM	Information Security	ISM.XML.V2015-Aug	XML Data Encoding Specification for Information Security Markings, Version, 2015-AUG
IC-EDH	Information Security	IC-EDH.XML.V4	XML Data Encoding Specification for Enterprise Data Header, Version 2015-AUG

UNCLASSFIED	
Electronic Records Management (ERM)	
Metadata Tag	***Description***
erm:AppliedBy	Individual that performed the disposition of the Record.
erm:Authorizer	Entity responsible for the hold.
erm:DateApplied	Date when action was taken or applied to the Record.
erm:DateEligible	Date the record is eligible for disposition.
erm:DateLimit	Date by which a disposition action must be taken regarding the Record.
erm:Dispositoin	An action taken with regard to U.S. federal records that are no longer needed for current government business as determined by their appraisal pursuant to legislation, regulation, or administrative procedure.
erm:EffectiveDate	Date the hold order was effective.
erm:ElectronicRecordsManagementMetadata	Information used by a records management system to manage a resource. A records management system systematically controls the creation, distribution, use, maintenance, and disposition of recorded information maintained as evidence of business activities and transactions.
erm:FoiaOpsIndicator	Indicator stating if the Record is exempted from FOIA search and publication (e.g. operations exemption at CIA): each agency has specific exemptions they request and maintain.
erm:Hold	A suspension of disposition of a set of one or more records in the records management process of the cognizant organization or institution.
erm:Identifier	Specific way to identify the hold (unique among hold types and agencies).
erm:Justification	Legal, policy, or mission driver for the hold order.

UNCLASSFIED	
Electronic Records Management (ERM)	
Metadata Tag	***Description***
erm:OfficeOfRecord	Identifies the Agency and organization element within the agency that is responsible for making decisions related to the Record. Also identifies which organizational element within an agency owns/is responsible for the official copy of the Record.
erm:RecordControl	Identifier for Agency Record Control System (RCS) disposition policies (per NARA).
erm:RecordDesignationDate	Date the Record is declared final (e.g. cutoff, publication, creation) and starts the retention period which will be used to calculate the disposition date based on the retention schedule.
erm:ReleasedDate	Date the hold order was released.
erm:ReviewIndicator	Indicator stating that the resource has been reviewed to determine the appropriate RCS, if applicable.
erm:Type	The category of a hold on a managed Record's disposition.
erm:VitalRecordsIndicator	Indicator stating that the Record is a Vital Record. Vital Records are those Records considered essential to the continuity of operation during and after emergencies or disaster conditions. Also known as Essential Records (per Federal Continuity Directive 1 (FCD 1)

G-G.2 TRUSTED DATA FORMAT (TDF) (REVISED!)

Trusted Data Format (TDF) is an IC mandatory standard and is identified as the way ahead strategy for implementing cloud-based information exchange and discovery on the IC enterprise. It is the metadata envelope or wrapper to transmit a data object or a reference to a data object.

The Trusted Data Format (TDF) specification is found in the following location within the IC Technical Specifications Library:

https://intelshare.intelink.ic.gov/sites/odni/cio/me/techspecs/Documents/ic-tdf/default.aspx

TDF has a dependency with the standards show in the following table:

UNCLASSFIED			
TDF Dependent Standards			
Abbreviation	***Category***	***ID***	***Title***
ISM	Information Security	ISM.XML.V2015-Aug	XML Data Encoding Specification for Information Security Markings, Version, 2015-AUG
NTK	Information Security	NTK.XML.V2015-AUG	XML Data Encoding Specification for Need-to-Know Metadata, Version 2015-AUG
IC-EDH	Information Resource	IC-EDH.XML.V2015-AUG	XML Data Encoding Specifications for Enterprise Data header, Version 2015-AUG
ARH	Information Security	ARH.XML.V3	XML Data Encoding Specification for Access Rights and Handling, Version 3, 6 September 2013
RevRecall	Information Resource	REVRECALL.XML.V1	XML Data Encoding Specification for Revision Recall, Version 1, 10 March 2014

The following table provides definitions of the primary TDF concepts.

Concept	*Description and Business Rules*
Trusted Data Object (TDO)	A Trusted Data Object (TDO) is the basic building block and contains one or more assertions (statement about the data) and the payload data. A TDO can be used at the very minimum to specify payload and assertions for a single payload item. The basic structure of a TDO is the following: <TrustedDataObject> <tdf:HandlingAssertion `tdf:scope="TDO"`> <tdf:HandlingStatement> <edh:ExternalEDH/> <arh:Security..> <ntk:Access…/> <arh:Security../> </edh:ExternalEDH/> <tdf:HandlingStatement/> </tdf:HandlingAssertion> <tdf:Assertion `tdf:scope="PAYL"`> <tdf: ReferenceValuePayload `tdf:uri="http://example/reference/payload"/`> 1 (one) </tdf:Assertion> </TrustedDataObject> 1. Note the use of the HandlingAssertion scope attribute to refer the scope of the handling assertion for the “TDO”.

Concept	Description and Business Rules
	2. Note the use of the Assertion scope attribute to refer to the scope of the assertion for the “PAYL. 3. Note the use of the ExternalEDH element to refer to an external. 4. Note the use of ReferenceValuePayload element to refer to an external reference to the payload item.

Concept	*Description and Business Rules*
Trusted Data Collection (TDC)	A Trusted Data Collection (TDC) is a collection of Trusted Data Objects (TDOs) used to assemble more than one payload item that can be related or unrelated and contains one or more The basic structure of a TDC is the following: <TrustedDataCollection> <tdf:HandlingAssertion tdf:scope="TDC"> <tdf:HandlingStatement> <edh:ExternalEDH/> <arh:Security..> <ntk:Access…/> <arh:Security../> </edh:ExternalEDH/> <tdf:HandlingStatement/> </tdf:HandlingAssertion> <TrustedDataObject> <tdf:Assertion/> … </TrustedDataObject> </TrustedDataCollection> 1. Note the use of the HandlingAssertion scope attribute to refer the scope of the handling assertion for the “TDC”.

Concept	*Description and Business Rules*
Handling Assertion	A handling assertion is a statement about the access, rights, and handling instructions of the payload. *As shown in the TDO structure example above,* • At least one handling instruction is required for each TrustedDataCollection (TCO) or TrustedDataObject (TDO) • An EDH and related security attributes are included in a handling assertion. • Definitions of EDH and related security attributes are defined in the EDH section. A handling assertion: • is never encrypted. • can include a Revision Recall handling assertion. • is made before other assertions in the document order *as shown in the TDO and TCO examples*. • can include XML, binary, and by reference, formats.
Handling Assertion Scopes	A handling assertion is identified by the tdf:HandlingAssertion element and will contain an attribute scope (@type:scope). The scope attribute of the handling assertion will specify the scope of the handling assertion (“TDC”, “DES_TDO”, “DESC_PAYL”). Additional information for assertion scopes is found in Section 2.3 of the specification. See section 2.3.1.2 Assertion Scopes within the TDC for additional scopes and definitions.

Concept	*Description and Business Rules*
Other Assertion or Mission Assertion	Other assertions or mission assertions are a statement about the payload that are not handling assertions and relate to the mission, discovery, or task order, etc. The Assertion attribute type is used to indicate the category of assertion that is intended, such as <Assertion @type=”Discovery”/>
Assertion Scopes (Mission and Other Assertions)	An assertion is identified by the tdf:Assertion element and will contain an attribute scope (@type:scope). The scope attribute of the handling assertion will specify the scope of the handling assertion (“TDO”, “PAYL”). Additional information for assertion scopes is found in Section 2.3 of the specification. See section 2.3.1.2 Assertion Scopes within the TDC for additional scopes and definitions.
Payload	Payload information includes the following formats: string, XML, binary, and by reference. The following TDF elements are used to convey the different payload: • StringPayload • Base64BinaryPayload • ReferenceValuePayload • StructuredPayload

A sequential output of the primary TDF XML elements is shown in the following table:

UNCLASSFIED	
TDF	
TDF Element	*Description*
{tdf} IC-TDF-collection	The root element of a Trusted Data Collection. A TDC can have a single HandlingAssertion containing and ICEDH specification and its scope must be TDC. There may also be an optional second HandlingAssertion scope [TDC] that contains Revision/Recall information for the TDC using the RevRecall.XML specification. A HandlingAssertion must not be encrypted.
{TrustedDataCollection} tdf:HandlingAssertion	A specific type of assertion designed to be used for access, rights, and handling instructions. It is expected that handling instructions should never have metadata about themselves and they should never be encrypted. Therefore, unlike regular assertions, handling assertions do not support statement metadata or encryption.
{TrustedDataCollection, tdf:HandlingAssertion} attr:scope	The grouping of objects to which the assertion applies.
{TrustedDataCollection, tdf:HandlingAssertion} tdf:HandlingStatement	Intended for access, rights, and/or handling instructions that apply to the scope of the assertion.
{tdf} TrustedDataObject	A TDO has at a minimum two Handling Assertions: A TDO handling assertion and a payload handling assertion. This allows for separate access control decisions to be made for the payload versus the entire TDO (which includes payload metadata).
{TrustedDataObject} tdf:HandlingAssertion	A specific type of assertion designed to be used for access, rights, and handling instructions. It is expected that handling instructions should never have metadata about themselves and they should never be encrypted. Therefore, unlike regular assertions, handling assertions do not support statement metadata or encryption.

UNCLASSFIED	
TDF	
TDF Element	*Description*
{TrustedDataObject} tdf: Assertion	Used to express metadata about the objects expressed in the scope attribute of the assertion. An assertion also supports metadata about the assertion statement for the purposes of indicating any handling instructions pertinent to the statement itself. Also supports encrypted statements and binding the statement with objects in its scope.
{TrustedDataObject, tdf: Assertion}attr:scope	The grouping of objects to which the assertion applies.
{TrustedDataObject, tdf: Assertion} tdf:StringStatement	Intended for textual statement content encoded as a string. Perhaps the contents of a text file.
{TrustedDataObject, tdf:Assertion} tdf:Base64BinaryStatement	Intended for holding base64binary statement values such as a file or other binary encoded data.
{TrustedDataObject, tdf:Assertion} tdf:ReferenceValuePayload	Used to reference payloads that are not embedded in the TDO but stored in a remote/external location.

G-G.3 IC Enterprise Data Header (IC-EDH)

IC Enterprise Data Header (EDH) is an XML encoding standard intended to allow interoperability and data sharing by establishing a core set of universal identity and categorization metadata attributes, for all stored data. As part of and along with the data exchange standard Trusted Data Format (TDF), it provides the common XML elements and structure needed in the enterprise to exchange and store information, including exchanges between systems and cloud based environments.

The IC-EDH specification is found at the following location: https://intelshare.intelink.ic.gov/sites/odni/cio/me/techspecs/Documents/ic-edh/default.aspx

IC-EDH has a dependency with the standards show in the following table.

UNCLASSFIED			
IC-EDH Dependent Standards			
Abbreviation	*Category*	*ID*	*Title*
IC-ID	Information Resource	IC-ID.XML.V1	XML Data Encoding Specification for Intelligence Community Identifier Metadata, Version 1, 10 April 2013
ARH	Information Security	ARH.XML.V3	XML Data Encoding Specification for Access Rights and Handling, Version 3, 6 September 2013
ISM	Information Security	ISM.XML.V2015-Aug	XML Data Encoding Specification for Information Security Markings, Version, 2015-AUG
NTK	Information Security	NTK.XML.V2015-AUG	XML Data Encoding Specification for Need-to-Know Metadata, Version 2015-AUG
ISMCAT	Information Security	ISMCAT.CES.V2016-May	XML Controlled Vocabulary Encoding Specification for ISM Country Codes and Tetragraphs, Version 2016-MAY
US Agency	Information Resource	USGOVAgency.CES.V2014-Sep	XML Controlled Vocabulary (CVE) Encoding Specification Government Agency Acronyms, Version 2014-SEP, 01 September 2014

The complete list of EDH elements and definitions are shown in the following table.

The namespace for each of the representative standards is shown for the element along with the parent-child relationship.

UNCLASSFIED	
IC-EDH	
EDH Element	***Description***
{edh:ExternalEDH} edh:ExternalEDH	Used for specifying an object's basic header information required for exchange on the IC Enterprise when the object is not in the instance document that this element is used. Values specified in this header will not contribute to roll-up.

EDH Element	*Description*
{edh:ExternalEDH} ntk:DESVersion	e.g. 201508
{edh:ExternalEDH} ism:DESVersion	e.g. 201508
{edh:ExternalEDH} ism:ISMACTESVersion	e.g. 20105
{edh:ExternalEDH} arh:DESVersion	e.g. 3
{edh:ExternalEDH} edh:DESVersion	e.g. 201508
{edh:ExternalEDH} edh:DataItemCreateDate	e.g. 2006-05-04T18:13:51.0Z
{edh:ExternalEDH} edh:AuthorizationReference	Attribute to hold the authorization reference of the data object referred to by the EDH. One or more indicators of a unique and documented legal basis for all activities surrounding the creation, retention and use of an information resource.
{edh:ExternalEDH} edh:AuthorizationReferenceType	One or more indicators of a unique and documented legal basis for all activities surrounding the creation, retention and use of an information resource.
{edh:ExternalEDH} edh:ResponsibleEntity	The creator entity that created the data item referenced by the EDH.
{edh:ExternalEDH, edh:ResponsibleEntity,ism:SecurityAttributesGroup} ism:atomicEnergyMarkings	Applicable atomic energy information markings for a document or portion This attribute is used at both resource and portion levels. The permissible values for this simple type are defined in the ISM Atomic Energy Markings CVE: CVEnumISMAtomicEnergyMarkings.xml. Applicable atomic energy information markings for a document or portion This attribute is used at both resource and portion levels. The permissible values for this simple type are defined in the ISM

EDH Element	*Description*
	Atomic Energy Markings CVE: CVEnumISMAtomicEnergyMarkings.xml.
{edh:ExternalEDH, edh:ResponsibleEntity,ism:SecurityAttributesGroup} ism:classification	The highest level of classification applicable to the containing document or portion The Classification element is always used in conjunction with the Owner Producer element. Taken together, the two elements specify the classification category (TS, S, C, R, or U) and the type of classification (US, non-US, or Joint). This attribute is used to render portion marks and security banners. This attribute is used at both resource and portion levels. The permissible values for this simple type are defined in the ISM Classification All CVE: CVEnumISMClassificationAll.xml
{edh:ExternalEDH, edh:ResponsibleEntity,ism:SecurityAttributesGroup} ism:classificationReason	One or more reason indicators or explanatory text describing the basis for an original classification decision This attribute corresponds to the “Reason” line of a document’s classification authority block, and it is only used, and only allowed, when classification is the result of an original classification decision. It is used primarily at the

EDH Element	*Description*
	resource level.
{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttributesOptionGroup} ism:classifiedBy	The identity, by name or personal identifier and position title, of the original classification authority for a document This attribute corresponds to the “Classified By” line of a resource’s classification authority block. It is used primarily at the resource level.
{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttributesOptionGroup} ism:compilationReason	The reason that the classification of the document is more restrictive than the simple roll-up of the marked portions of the document This attribute is an indicator that there is not accidental over-classification of the document. Users must exercise special care beyond that indicated by the portion marks when using this information.
{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttributesOptionGroup} ism:declassDate	The specific date when the resource is subject to automatic declassification procedures if not properly exempted from automatic declassification This attribute corresponds to the “Declassify On” line of a resource’s classification authority block. It is used primarily at the resource level.

EDH Element	*Description*
{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttributesOptionGroup} ism:declassEvent	A description of an event upon which the information shall be subject to automatic declassification procedures if not properly exempted from automatic declassification A description of an event upon which the information shall be automatically declassified if not properly exempted from automatic declassification. This attribute corresponds to the “Declassify On” line of a resource’s classification authority block. It is used primarily at the resource level.
{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttributesOptionGroup} ism:declassException	The exemption from automatic declassification that is claimed for a document This element is used in conjunction with the Declassification Date or Declassification Event, and it corresponds to the “Declassify On” line of a resource’s classification authority block. It is used primarily at the resource level. The permissible values for this attribute are defined in the ISM N25X CVE: CVEnumISMN25X.xml. ISOO Guidance: @declassException should be a SINGLE value giving the longest protection.
{edh:ExternalEDH, edh:ResponsibleEntity, ism:SecurityAttributesGroup} ism:derivativelyClassifiedBy	The identity, by name or personal identifier, of the derivative classification authority This attribute corresponds to the “Classified By” line of a resource’s classification authority block, and it is used primarily at the resource level.

EDH Element	*Description*
{edh:ExternalEDH, edh:ResponsibleEntity,ism:SecurityAttributesGroup} ism:derivedFrom	A citation of the authoritative source or sources of the classification markings used in a derivative classification decision for a classified document This attribute corresponds to the “Derived From” line of a document’s classification authority block, and it is used primarily at the resource level. ISOO Guidance: The source of derivative classification. (1) The derivative classifier shall concisely identify the source document or the classification guide on the ‘‘Derived From’’ line, including the agency and, where available, the office of origin, and the date of the source or guide. An example might appear as: Derived From: Memo, ‘‘Funding Problems,’’ October 20, 2008, Office of Administration, Department of Good Works or Derived From: CG No. 1, Department of Good Works, dated October 20, 2008 (i) When a document is classified derivatively on the basis of more than one source document or classification guide, the ‘‘Derived From’’ line shall appear as: Derived From: Multiple Sources (ii) The derivative classifier shall include a listing of the source materials on, or attached to, each derivatively classified document.
{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttributesOptionGroup} ism:displayOnlyTo	The set of countries and/or international organizations associated with a “Display Only To” marking The “Display Only To” marking indicates that a document is authorized for foreign viewing by appropriate affiliates of approved countries and/or international organizations without providing the foreign recipient with a copy for retention in any medium (physical or electronic). This attribute is used at both the resource and the portion levels.

EDH Element	*Description*
	The permissible values for this attribute are defined in the ISM Rel To CVE: CVEnumISMRelTo.xml.
{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttributesOptionGroup} ism:disseminationControls	Applicable dissemination control markings for a document or portion This attribute is rendered in portion marks and banners. The permissible values for this attribute are defined in the ISM Dissemination CVE: CVEnumISMDissem.xml
{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttributesOptionGroup} ism:FGIsourceOpen	The set of countries and/or international organizations whose information is derivatively sourced in a document when the source of the information is not concealed (also used for cases when the source is unknown) FGI markings protect foreign-owned or foreign-produced information and are applied based on sharing agreements or arrangements with the source country or organization. This attribute is used at both the resource and the portion levels. The permissible values for this attribute are defined in the ISM FGI Open CVE: CVEnumISMFGIOpen.xml. Note: the value “UNKNOWN” is allowed in cases where the source of the information is not known.

EDH Element	*Description*
{edh:ExternalEDH, edh:ResponsibleEntity, ism:SecurityAttributesOptionGroup} ism:FGISourceProtected	The set of countries and/or international organizations whose information is derivatively sourced in a document when the source of the information must be concealed This attribute has specific rules concerning its usage: PROTECTED SPACES — Within protected internal organizational spaces, this attribute may be used to maintain a formal record of the foreign country or countries and/or registered international organization(s) that are the non-disclosable owner(s) and/or producer(s) of information which is categorized as foreign government information according to Security Markings Program guidelines. If the data element is employed in this manner, then additional measures must be taken prior to dissemination of the resource to shared spaces so that any indications of the non-disclosable owner(s) and/or producer(s) of information within the resource are eliminated. In all cases, the corresponding portion marking or banner marking should be compliant with Security Markings Program guidelines for FGI when the source must be concealed. In other words, even if the data element is being employed within protected internal organizational spaces to maintain a formal record of the non-disclosable owner(s) and/or producer(s) within an XML resource, if the resource is rendered for display within the protected internal organizational spaces in any format by a stylesheet or as a result of any other transformation process, then the non-disclosable owner(s) and/or producer(s) should not be included in the corresponding portion marking or banner marking. SHARED SPACES — Within shared spaces, the data element serves only to indicate the presence of FGI; in this case, this element’s value will always be “FGI”. The data element may also be employed in this manner within protected internal

EDH Element	Description
	organizational spaces. Permissible values for this attribute are defined in the ISM FGI Protected CVE: CVEnumISMFGIProtected.xml. Note: the value “FGI” is permitted in the case outlined for “shared spaces”.

EDH Element	*Description*
{edh:ExternalEDH, edh:ResponsibleEntity, ism:SecurityAttributesOptionGroup} ism:joint	When true, an indicator that entities in the @ism:ownerProducer attribute are JOINT owners of the data
{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttributesOptionGroup} ism:Nonicmarkings	One or more indicators of an expansion or limitation on the distribution of a document or portion originating from non-intelligence components This attribute is used at both the resource and the portion levels, and it is rendered in portion marks and security banners. The permissible values for this attribute are defined in the ISM Non-IC CVE: CVEnumISMNonIC.xml
{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttributesOptionGroup} ism:Nonuscontrols	One or more indicators of an expansion or limitation on the distribution of a document or portion originating from non-US components (foreign government or international organization). This attribute is used at both the resource and the portion levels, and it is rendered in portion marks and security banners. The permissible values for this attribute are defined in the ISM Non-US Controls CVE: CVEnumISMNonUSControls.xml
{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttributesOptionGroup} ism:OwnerProducer	The set of national governments and/or international organizations that have purview over the containing classification marking This element is always used in conjunction with the Classification element. Taken together, the two elements specify the classification category (TS, S, C, R, or U) and the type of classification (US, non-US, or Joint). The permissible values for this attribute are defined in the ISMCAT Owner Producer CVE: CVEnumISMCATOwnerProducer.xml.

EDH Element	*Description*
{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttributesOptionGroup} ism:releasableTo	This attribute is used at both the resource and the portion levels. One or more indicators identifying the country or countries and/or international organization(s) to which classified information may be released based on the determination of an originator in accordance with established foreign disclosure procedures. This element is used in conjunction with the Dissemination Controls element. It is manifested in portion marks and security banners. PERMISSIBLE VALUES The permissible values for this attribute are defined in the Controlled Value Enumeration: CVEnumISMRelTo.xml
{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttributesOptionGroup} ism:SARIdentifier	This attribute is used at both the resource and the portion levels. One or more indicators identifying the defense or intelligence programs for which special access is required. It is manifested in portion marks and security banners. PERMISSIBLE VALUES The permissible values for this attribute are defined in the Controlled Value Enumeration: CVEnumISMSAR.xml
{edh:ExternalEDH, edh:ResponsibleEntity} ism:SecurityAttributesOptionGroup	This attribute is used at both the resource and the portion levels. One or more indicators identifying sensitive compartmented information control system(s). It is manifested in portion marks and security banners. PERMISSIBLE VALUES The permissible values for this attribute are defined in the Con- trolled Value Enumeration: CVEnumISMSCIControls.xml
{edh:ExternalEDH,edh:ResponsibleEntity} edh:Country	The ISO 3166 country code of the organization that created the data item.
{edh:ExternalEDH,edh:ResponsibleEntity} edh:Organization	The organization within the country specified that created the data item.
{edh:ExternalEDH,edh:ResponsibleEntity} edh:Suborganization	The sub organization within the organization specified that created the data item.
{edh:ExternalEDH} edh:DataSet	A means of indicating a particular association of data. MUST not impact access control, access control MUST be entirely

EDH Element	*Description*
	contained in the ARH section.
{edh:ExternalEDH,arh:ExternalSecurity} ism:compliesWith	e.g. compliesWith="USGov USIC
{edh:ExternalEDH,arh:ExternalSecurity} ism:resourceElement	e.g. TRUE
{edh:ExternalEDH,arh:ExternalSecurity} ism:createDate	e.g. 5/4/206
{edh:ExternalEDH,arh:ExternalSecurity} ism:classification	e.g. U
{edh:ExternalEDH,arh:ExternalSecurity} ism:ownerProducer	e.g. USA
{edh:ExternalEDH,arh:ExternalSecurity} ism:excludeFromRollup	e.g. TRUE
{edh:ExternalEDH,ntk:ExternalAccess}	A way of describing a formalized Need to Know required for a document. NTK requires being inside a schema that implements ISM therefore some element in the implementing schema MUST have ism:ISMRootNodeAttributeGroup and ism:ResourceNodeAttributeGroup since both of those are required for a valid ISM implementation. In addition the root node of the implementing schema must have ntk:NTKRootNodeAttributeGroup specified
{edh:ExternalEDH,ntk:ExternalAccess} ntk:externalReference	e.g. TRUE
{edh:ExternalEDH,ntk:ExternalAccess} ism:classification	e.g. U
{edh:ExternalEDH,ntk:ExternalAccess} ism:ownerProducer	e.g. USA

EDH Element	*Description*
{edh:ExternalEDH,ntk:ExternalAccess} ntk:AccessProfile	An access policy name followed by 1 or more values representing a profile that a user wanting access to the document must meet. Logic for the profile list being Boolean AND vs OR is Access Policy defined.
{edh:ExternalEDH,ntk:ExternalAccess} ntk:RequiresAllOf	A logical grouping indicating that all included access policies are required.
{edh:ExternalEDH,ntk:ExternalAccess} ntk:RequiresAnyOf	A logical grouping indicating that one of the included access policies is required.
{edh:ExternalEDH,ntk:ExternalAccess, ism:NoticeExternal}	A single Notice that may consist of 1 or more NoticeText for use when the notice refers to something external.
{edh:ExternalEDH,ntk:ExternalAccess, ism:NoticeExternal} ism:externalNotice	The actual notice of a text.

APPENDIX G-H: NGA METADATA PROFILE

The following table is a sequential output of all the data elements are represented as NGA required fields and IC required standards in order or relevance:

- National Metadata Foundation (NMF)
- Additional per feedback per CDO, A, S, and X
- Electronic Rights Management (ERM)
- Trusted Data Format (TDF)
- IC Enterprise Data Header (IC-EDH)

UNCLASSFIED		
NGA Metadata Profile		
Metadata Point of Contact	NMF 3.0	The party or parties acting in a role of responsibility for a set of resource metadata.
Metadata Date	NMF 3.0	The date(s), and optionally time(s), of an event involving a set of resource metadata.
Metadata Standard Title	NMF 3.0 A&S	The name of the metadata standard which determines the structure and content of this set of resource metadata.
Metadata Standard Edition	NMF 3.0 A&S	The version of the metadata standard which determines the structure and content of this set of resource metadata.
Metadata Scope Code	NMF 3.0	A brief indicator of the type of resource for which metadata information is reported.
Metadata Scope Name	NMF 3.0	A word or phrase that describes the type of resource for which information is reported.
Metadata Classification	NMF 3.0	The classification level of the metadata, in accordance with the Intelligence Community (IC) Security Markings Manual.
Metadata Classification System	NMF 3.0	The classification system of the metadata, in accordance with the Intelligence Community (IC) Security Markings Manual.
Resource Title	NMF 3.0	The name by which a cited resource is known.

UNCLASSFIED		
NGA Metadata Profile		
Resource Abstract	NMF 3.0 A&S X	A brief statement or narrative summary of the resource.
{edh:ExternalEDH}edh :ResponsibleEntity **{NMF} Resource Point of Contact**	EDH NMF 3.0 A&S X	The party(ies) acting in a role of responsibility for the resource.
{edh:ExternalEDH}edh:DataItemCreateDate **{NMF} Resource Date**	EDH NMF 3.0 A&S	A reference date for a cited resource. The first instance of this element is to have the role of “creation”.
{edh:ExternalEDH} icid:Identifier **{NMF} Resource Identifier**	NMF 3.0 EDH A&S	A value uniquely identifying the resource within a namespace.
Resource Geographic Location	NMF 3.0 A&S	The spatial extent of the resource. The spatial extent is a geographic identifier (for example: a country name), a bounding box (for example: the bounding latitudes and longitudes), or a bounding object (for example: a set of coordinate points).
Resource Language	NMF 3.0 A&S	Designation of the locale language.
Resource Character Set	NMF 3.0	Designation of the character set to be used to encode the textual value of the locale.
Resource Topic Category Code	NMF 3.0 A&S X	A theme or topic keyword that represents a subject of the resource.

Resource Keywords	NMF 3.0 A&S X	Information about keywords describing this resource.
{edh:ExternalEDH, edh:ResponsibleEntity, ism:SecurityAttributesOptionGroup}ism:classification **{NMF} Resource Classification**	EDH NMF 3.0	The classification level of the resource, in accordance with the Intelligence Community (IC) Security Markings Manual.
{edh:ExternalEDH, edh:ResponsibleEntity, ism:SecurityAttributesOptionGroup}ism:derivedFrom **{NMF} Resource Classification System**	EDH NMF 3.0 A&S	The classification system of the resource, in accordance with the Intelligence Community (IC) Security Markings Manual.
Resource Category	NMF 3.0	The particular category of a data resource within a defined taxonomy.
Metadata Language	NMF 3.0	Designation of the locale language.
Metadata Character Set	NMF 3.0	Designation of the character set to be used to encode the textual value of the locale
Parent Metadata Citation	NMF 3.0	A standardized reference to a set of metadata that is in a parent relationship to this set of resource metadata
Resource Temporal Extent	NMF 3.0 A&S	The time period covered by the resource
Resource Coordinate Reference System	NMF 3.0	Information about a spatial or temporal reference system used by representations in the resource.

UNCLASSFIED		
NGA Metadata Profile		
Content ID	NGA CDO	Number designated by the NGA to label content type.
Maintenance Cycle/Update Frequency	X	Indicates how of then the object is updated
Online Resource	A&S X	information about on-line sources from which the dataset, can be obtained (hyperlink to object)
erm:AppliedBy	ERM	Individual that performed the disposition of the Record.
erm:Authorizer	ERM	Entity responsible for the hold.
erm:DateApplied	ERM	Date when action was taken or applied to the Record.
erm:DateEligible	ERM	Date the record is eligible for disposition.
erm:DateLimit	ERM	Date by which a disposition action must be taken regarding the Record.
erm:Dispositoin	ERM	An action taken with regard to U.S. federal records that are no longer needed for current government business as determined by their appraisal pursuant to legislation, regulation, or administrative procedure.
erm:EffectiveDate	ERM	Date the hold order was effective.
erm:ElectronicRecordsManagementMetadata	ERM	Information used by a records management system to manage a resource. A records management system systematically controls the creation, distribution, use, maintenance, and disposition of recorded information maintained as evidence of business activities and transactions.
erm:FoiaOpsIndicator	ERM	Indicator stating if the Record is exempted from FOIA search and publication (e.g. operations exemption at CIA): each agency has specific exemptions they request and maintain.
erm:Hold	ERM	A suspension of disposition of a set of one or more records in the records management process of the cognizant organization or institution.
erm:Identifier	ERM	Specific way to identify the hold (unique among hold types and agencies).

UNCLASSFIED		
NGA Metadata Profile		
erm:Justification	ERM	Legal, policy, or mission driver for the hold order.
erm:OfficeOfRecord	ERM	Identifies the Agency and organization element within the agency that is responsible for making decisions related to the Record. Also identifies which organizational element within an agency owns/is responsible for the official copy of the Record.
erm:RecordControl	ERM	Identifier for Agency Record Control System (RCS) disposition policies (per NARA).
erm:RecordDesignationDate	ERM	Date the Record is declared final (e.g. cutoff, publication, creation) and starts the retention period which will be used to calculate the disposition date based on the retention schedule.
erm:ReleasedDate	ERM	Date the hold order was released.
erm:ReviewIndicator	ERM	Indicator stating that the resource has been reviewed to determine the appropriate RCS, if applicable.
erm:Type	ERM	The category of a hold on a managed Record's disposition.
erm:VitalRecordsIndicator	ERM	Indicator stating that the Record is a Vital Record. Vital Records are those Records considered essential to the continuity of operation during and after emergencies or disaster conditions. Also known as Essential Records (per Federal Continuity Directive 1 (FCD 1)
{tdf} IC-TDF-collection	TDF	The root element of a Trusted Data Collection. A TDC can have a single HandlingAssertion containing and IC-EDH specification and its scope must be TDC. There may also be an optional second HandlingAssertion scope [TDC] that contains Revision/Recall information for the TDC using the RevRecall.XML specification. A HandlingAssertion must not be encrypted.

{TrustedDataCollection} tdf:HandlingAssertion	TDF	A specific type of assertion designed to be used for access, rights, and handling instructions. It is expected that handling instructions should never have metadata about themselves and they should never be encrypted. Therefore, unlike regular assertions, handling assertions do not support statement metadata or encryption.
{TrustedDataCollection, tdf:HandlingAssertion} attr:scope	TDF	The grouping of objects to which the assertion applies.
{TrustedDataCollection, tdf:HandlingAssertion} **tdf:HandlingStatement**	TDF	Intended for access, rights, and/or handling instructions that apply to the scope of the assertion.
{tdf} TrustedDataObject	TDF	A TDO has at a minimum two HandlingAssertions: A TDO handling assertion and a payload handling assertion. This allows for separate access control decisions to be made for the payload versus the entire TDO (which includes payload metadata).
{TrustedDataObject} tdf:HandlingAssertion	TDF	A specific type of assertion designed to be used for access, rights, and handling instructions. It is expected that handling instructions should never have metadata about themselves and they should never be encrypted. Therefore, unlike regular assertions, handling assertions do not support statement metadata or encryption.
{TrustedDataObject} tdf:Assertion	TDF	Used to express metadata about the objects expressed in the scope attribute of the assertion. An assertion also supports metadata about the assertion statement for the purposes of indicating any handling instructions pertinate to the statement itself. Also supports encrypted statements and binding the statement with objects in its scope.
{TrustedDataObject, tdf:Assertion}attr:scope	TDF	The grouping of objects to which the assertion applies.

{TrustedDataObject,tdf:EncryptionInformationGroup} **tdf:EncryptionInformation**	TDF	(U) Top level element for holding information related to the encryption of an assertion or payload. Multiple child KeyAccess and/or EncryptionMethod elements represent onion or layered encryption. In this case, the first child represents the outermost layer of encryption. WILL USE ALL INFORMATION IF NECESSARY.
{TrustedDataObject, tdf:Assertion} **tdf:ReferenceValuePayload**	TDF	Used to reference payloads that are not embedded in the TDO but stored in a remote/external location.
{edh:ExternalEDH} **edh:ExternalEDH**	EDH	Used for specifying an object's basic header information required for exchange on the IC Enterprise when the object is not in the instance document that this element is used. Values specified in this header will not contribute to roll-up.
{edh:ExternalEDH} **ntk:DESVersion**	EDH	e.g. 201508
{edh:ExternalEDH} **ism:DESVersion**	EDH	e.g. 201508
{edh:ExternalEDH} **ism:ISMACTESVersion**	EDH	e.g. 20105
{edh:ExternalEDH} **arh:DESVersion**	EDH	e.g. 3
{edh:ExternalEDH} **edh:DESVersion**	EDH	e.g. 201508
{edh:ExternalEDH} **icid:Identifier** **or** **{NMF} Resource Identifier**	EDH NMF 3.0 A&S	e.g. guide://
{edh:ExternalEDH} **edh:DataItemCreateDate** **or**	EDH NMF A&S	e.g. 2006-05-04T18:13:51.0Z

{NMF} Resource Date		
{edh:ExternalEDH} edh:AuthorizationReference	EDH	Attribute to hold the authorization reference of the data object referred to by the EDH. One or more indicators of a unique and documented legal basis for all activities surrounding the creation, retention and use of an information resource.
{edh:ExternalEDH} edh:AuthorizationReferenceType	EDH	One or more indicators of a unique and documented legal basis for all activities surrounding the creation, retention and use of an information resource.
{edh:ExternalEDH} edh:ResponsibleEntity **or** **{NMF} Resource Point of Contact**	EDH NMF A&S X	The creator entity that created the data item referenced by the EDH.
{edh:ExternalEDH, edh:ResponsibleEntity,ism:SecurityAttributesGroup} ism:atomicEnergyMarkings	EDH	Applicable atomic energy information markings for a document or portion
{edh:ExternalEDH, edh:ResponsibleEntity,ism:SecurityAttributesGroup} ism:classification **or** **{NMF} Resource Classification**	EDH NMF	The highest level of classification applicable to the containing document or portion

{edh:ExternalEDH, edh:ResponsibleEntity,ism:SecurityAttributesGroup} **ism:classificationReason**	EDH	One or more reason indicators or explanatory text describing the basis for an original classification decision
{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttributesOptionGroup} **ism:classifiedBy**	EDH	The identity, by name or personal identifier and position title, of the original classification authority for a document
{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttributesOptionGroup} ism:compilationReason	EDH	The reason that the classification of the document is more restrictive than the simple roll-up of the marked portions of the document
{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttributesOptionGroup} **ism:declassDate**	EDH	The specific date when the resource is subject to automatic declassification procedures if not properly exempted from automatic declassification
{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttributesOptionGroup} ism:declassEvent	EDH	A description of an event upon which the information shall be subject to automatic declassification procedures if not properly exempted from automatic declassification A description of an event upon which the information shall be automatically declassified if not properly exempted from automatic declassification.
{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttributesOptionGroup} **ism:declassException**	EDH	The exemption from automatic declassification that is claimed for a document

{edh:ExternalEDH, edh:ResponsibleEntity, ism:SecurityAttrib-utesGroup} ism:derivativelyClassifiedBy	EDH	The identity, by name or personal identifier, of the derivative classification authority
{edh:ExternalEDH, edh:ResponsibleEntity,ism:SecurityAttributesGroup} ism:derivedFrom **{NMF} Resource Classification System**	EDH NMF	A citation of the authoritative source or sources of the classification markings used in a derivative classification decision for a classified document
{edh:ExternalEDH, edh:ResponsibleEntity,ism:SecurityAttributesGroup} ism:displayOnlyTo	EDH	The set of countries and/or international organizations associated with a “Display Only To” marking
{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttributesOptionGroup} ism:disseminationControls	EDH A&S	Applicable dissemination control markings for a document or portion
{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttributesOptionGroup} ism:FGIsourceOpen	EDH	The set of countries and/or international organizations whose information is derivatively sourced in a document when the source of the information is not concealed (also used for cases when the source is unknown)
{edh:ExternalEDH, edh:ResponsibleEntity, ism:SecurityAttributesOptionGroup} ism:FGISourceProtect	EDH	The set of countries and/or international organizations whose information is derivatively sourced in a document when the source of the information must be concealed

ed		
{edh:ExternalEDH, edh:ResponsibleEntity , ism:SecurityAttributes OptionGroup} **ism:joint**	EDH	When true, an indicator that entities in the @ism:ownerProducer attribute are JOINT owners of the data
{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttr ibutesOptionGroup} **ism:Nonicmarkings**	EDH	One or more indicators of an expansion or limitation on the distribution of a document or portion originating from non-intelligence components This attribute is used at both the resource and the portion levels, and it is rendered in portion marks and security banners. The permissible values for this attribute are defined in the ISM Non-IC CVE: CVEnumISMNonIC.xml
{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttr ibutesOptionGroup} **ism:Nonuscontrols**	EDH	One or more indicators of an expansion or limitation on the distribution of a document or portion originating from non-US components (foreign government or international organization).
{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttr ibutesOptionGroup} **ism:OwnerProducer**	EDH	The set of national governments and/or international organizations that have purview over the containing classification marking

{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttributesOptionGroup} ism:releasableTo	EDH A&S	This attribute is used at both the resource and the portion levels. One or more indicators identifying the country or countries and/or international organization(s) to which classified information may be released based on the determination of an originator in accordance with established foreign disclosure procedures. This element is used in conjunction with the Dissemination Controls element. It is manifested in portion marks and security banners. PERMISSIBLE VALUES The permissible values for this attribute are defined in the Controlled Value Enumeration: CVEnumISMRelTo.xml
{edh:ExternalEDH,edh:ResponsibleEntity,ism:SecurityAttributesOptionGroup} ism:SARIdentifier	EDH	This attribute is used at both the resource and the portion levels. One or more indicators identifying the defense or intelligence programs for which special access is required. It is manifested in portion marks and security banners. PERMISSIBLE VALUES The permissible values for this attribute are defined in the Controlled Value Enumeration: CVEnumISMSAR.xml
{edh:ExternalEDH, edh:ResponsibleEntity} ism:SecurityAttributesOptionGroup	EDH	This attribute is used at both the resource and the portion levels. One or more indicators identifying sensitive compartmented information control system(s). It is manifested in portion marks and security banners. PERMISSIBLE VALUES The permissible values for this attribute are defined in the Controlled Value Enumeration: CVEnumISMSCIControls.xml
{edh:ExternalEDH,edh:ResponsibleEntity} edh:Country	EDH	The ISO 3166 country code of the organization that created the data item.
{edh:ExternalEDH, edh:ResponsibleEntity} **edh:Organization**	EDH	The organization within the country specified that created the data item.

{edh:ExternalEDH,edh:ResponsibleEntity} edh:Suborganization	EDH	The suborganization within the organization specified that created the data item.
{edh:ExternalEDH} edh:DataSet	EDH	A means of indicating a particular association of data. MUST not impact access control, access control MUST be entirely contained in the ARH section.
{edh:ExternalEDH,arh:ExternalSecurity} ism:compliesWith	EDH	e.g. compliesWith="USGov USIC
{edh:ExternalEDH,arh:ExternalSecurity} ism:resourceElement	EDH	e.g. TRUE
{edh:ExternalEDH,arh:ExternalSecurity} ism:createDate	EDH	e.g. 5/4/206
{edh:ExternalEDH,arh:ExternalSecurity} ism:classification	EDH	e.g. U
{edh:ExternalEDH,arh:ExternalSecurity} ism:ownerProducer	EDH	e.g. USA
{edh:ExternalEDH,arh:ExternalSecurity} ism:excludeFromRollup	EDH	e.g. TRUE
{edh:ExternalEDH,ntk:ExternalAccess}	EDH	A way of describing a formalized Need to Know required for a document. NTK requires being inside a schema that implements ISM therefore some element in the implementing schema MUST have ism:ISMRootNodeAttributeGroup and ism:ResourceNodeAttributeGroup since both of those are required for a valid ISM implementation. In addition the root node of the implementing schema must have ntk:NTKRootNodeAttributeGroup specified

{edh:ExternalEDH,ntk:ExternalAccess} ntk:externalReference	EDH	e.g. TRUE
{edh:ExternalEDH,ntk:ExternalAccess} ism:classifi- cation	EDH	e.g. U
{edh:ExternalEDH,ntk:ExternalAccess} ism:ownerProducer	EDH	e.g. USA
{edh:ExternalEDH,ntk:ExternalAccess} ntk:AccessProfile	EDH	An access policy name followed by 1 or more values representing a profile that a user wanting access to the document must meet. Logic for the profile list being Boolean AND vs OR is Access Policy defined.
{edh:ExternalEDH,ntk:ExternalAccess} ntk:RequiresAllOf	EDH	A logical grouping indicating that all included access policies are required.
{edh:ExternalEDH,ntk:ExternalAccess} ntk:Re- quiresAnyOf	EDH	A logical grouping indicating that one of the included access policies is required.
{edh:ExternalEDH,ntk:ExternalAccess, ism:NoticeExternal}	EDH	A single Notice that may consist of 1 or more NoticeText for use when the notice refers to something external.
{edh:ExternalEDH,ntk:ExternalAccess, ism:NoticeExternal} ism:externalNotice	EDH	The actual notice of a text.

APPENDIX G-I: DATA IN THE CLOUD – EXAMPLE CASES

This section presents two example paths for evolving to the cloud architecture, to assist Data Stewards and Program Managers design a customized appropriate path for their own data. Both examples move from a current system architecture where data is tightly coupled to the applications (Activities) to a target architecture where the data is decoupled from the applications through the introduction of data services. Example one describes a potential path to evolve from a system that manages data objects with integrated (tightly coupled to the application) metadata management and access controls to a set of multipurpose enterprise data management and access and security services, using S3 as the storage service. Example two is similar but takes a database that uses Statefull client-server technology to a cloud based (C2S RDS) database using Restful services. Both paths balance moving the data to the cloud with minimizing the near term impact to the applications.

Representative 'real' Activities are used to allow for more vivid examples. But it should be understood that the details are somewhat notional and are under development as NCL and AMS continue to define their evolution paths as part of their respective cloud migration project planning and design efforts.

G-I.1 Data Storage Architecture Evolution – An Object Storage (S3) Example Case (REVISED!)

An example using the NSG Consolidated Library (NCL) illustrates data architecture evolution where the main data are objects – specifically, a large library of imagery. NCL has its own catalog of imagery metadata, its own sophisticated policy enforcement capabilities which can enforce access down to the pixel block level, its own image format, and transformation services.

NOTE: THE DIAGRAMS IN THIS SECTION ARE NOTIONAL - NOT MEANT TO REPRESENT ACTUAL PHYSICAL CONFIGURATIONS

Now – Current State

The OpenDataStore exists, but there are no PEPs defined, no established enterprise metadata catalog, and no enterprise Image Format Transformation services.

The NCL imagery is migrated to S3"Dirty Buckets" in the OpenDataStore (the NGA enterprise content account created by the CDO). Access to NCL imagery would still require access through the NCL activity.

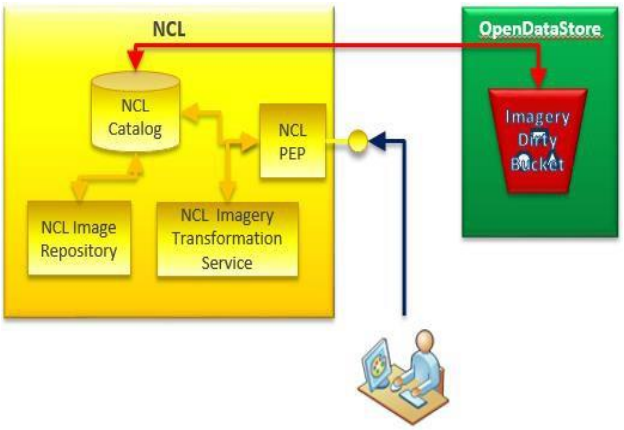


Figure I-0-1: S3 Now – Current State Architecture

Next – Transitional State

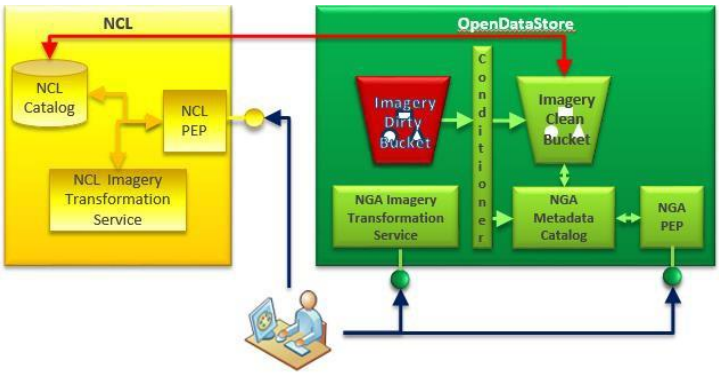


Figure I-0-2: S3 Next - Transitional

The NCL imagery in the “Dirty Buckets” will be conditioned (metadata tagged), and registered in the enterprise metadata catalog, which changes its status to a useable “clean” state. At this point, NCL and non-NCL users will be able to discover the imagery which has been conditioned and registered in the enterprise metadata catalog without using the NCL application. See the Metadata Guidance for more details on conditioning and the enterprise metadata catalog. NCL would operate as it had previously with the exception of having the data stored in the OpenDataStore.

Users could still use the NCL activity and its suite of services if desired, but with the following services implemented would not need to, taking the first step to truly separating the Application from the Data. Enterprise services would include:

- Enterprise PEP will be defined and business rules will be established to negotiate user access rights and data/metadata attributes. Initially enforcement

may only go to the file level, instead of pixel block level enforcement, but will allow access control without using the NCL application.

- Enterprise Imagery Format Transformation service. This could take any imagery in any format it supports and transform it to any other imagery format supported.

Target State

The enterprise services would continue to improve, to include achieving the same pixel block level policy enforcement available in NCL today.

NCL would transition from using its own PEP, Metadata Catalog and Imagery Transformation suite of services, and use the available enterprise services instead.

What remains in NCL would be services unique to it, such as the user interface and reports.

One architectural objective is to separate the data from the Activity. To this end, the architecture includes the services needed to discover, access and transform the data for use by anyone or activity in the NSG enterprise.

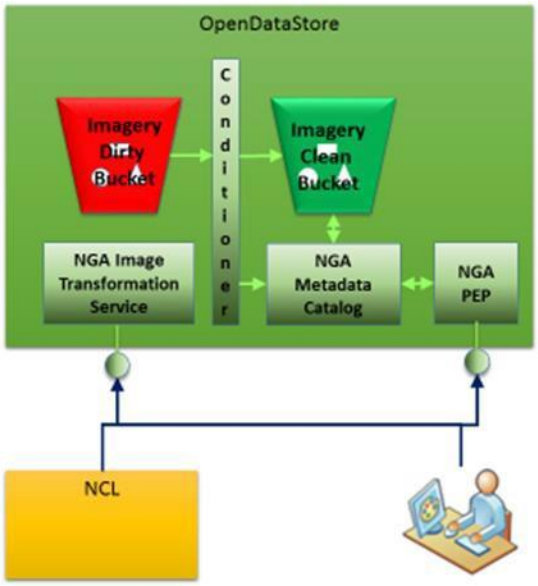


Figure I-0-3: Cloud OpenDataStore, S3 Target State

G-I.2 Data Storage Architecture Evolution – A Database (RDB) Example Case

The Aeronautical Migration System (AMS) is the production system for Aeronautical Safety of Navigation (SoN). It is subject to intense international regulations to enable the data to be used in aircraft Flight Management Systems (FMS, aka Autopilot). To maintain their current certification, they are audited every 6 months. If they change technologies significantly, it will require a completely new certification, which could take over a year after the new development is completed.

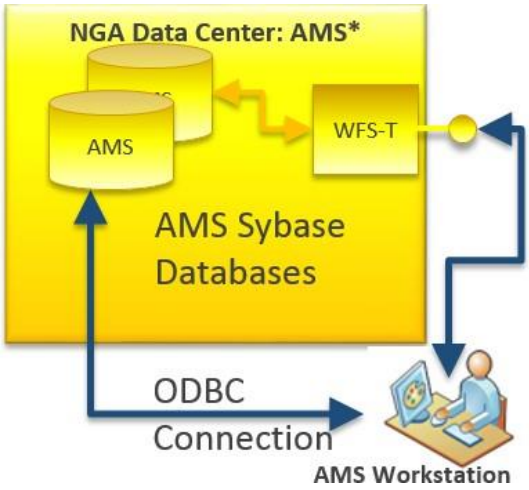


Figure I-0-4: Database As-Is Example

The current AMS system is client-server based, with Sybase Databases, Visual Basic 5 & 6 Clients, and a Boundless OpenGeo QGIS client. The Visual Basic clients connect via ODBC directly to the database. The OpenGeo QGIS client connects via an OGC Transactional Web Feature Service (WFS-T). Visual Basic clients need to be maintained to support non-spatial data.

Option 1: Re-host Sybase

The easiest Cloud Migration option is re-hosting setting up an EC2/EBS instance in the OpenDataStore and recreate the existing Sybase Databases. This will maintain their current, legacy functionality without triggering a recertification of AMS because the software technology stack is unchanged. However, other than getting AMS out of the NGA Data Center, substantial benefits are unlikely.

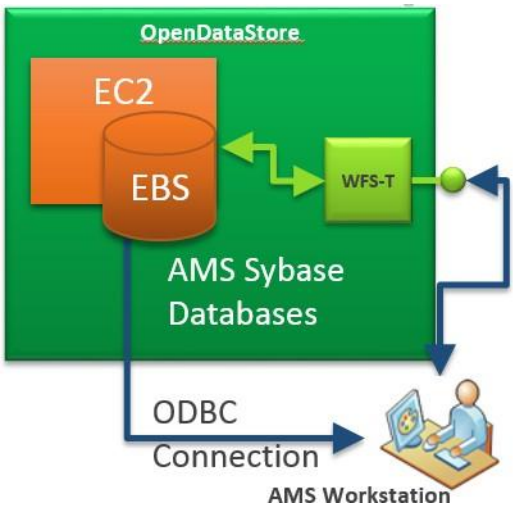


Figure I-0-5: Option 1 - Lift & Shift Rehost

Option 2: Migrate to RDS

Aeronautical has been contemplating updating to a more modern database and identified PostgreSQL with PostGIS as the best candidate. They intend to consolidate their Sybase databases into a unified C2S RDS PostgreSQL database. This is a significant transformation. It will allow transitioning away from the ODBC connection, and represents a significant cost savings not only in licensing costs (PostgreSQL is open source) but in maintenance resources that should not be required in C2S RDS. However, they cannot use the new system to produce Aeronautical SoN products without recertifying the system, which will take over a year after development is complete.

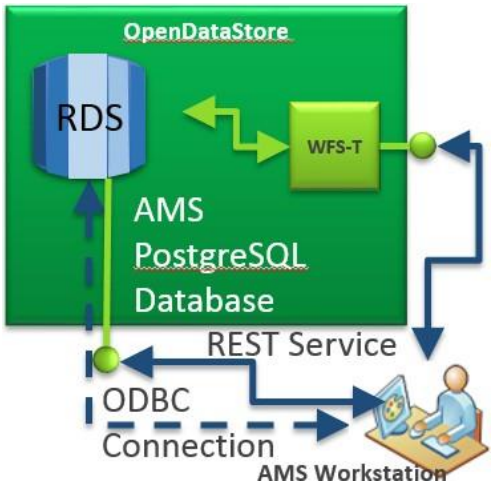


Figure I-0-6: Option 2 RDS

Option 3: Phased Combined Solution

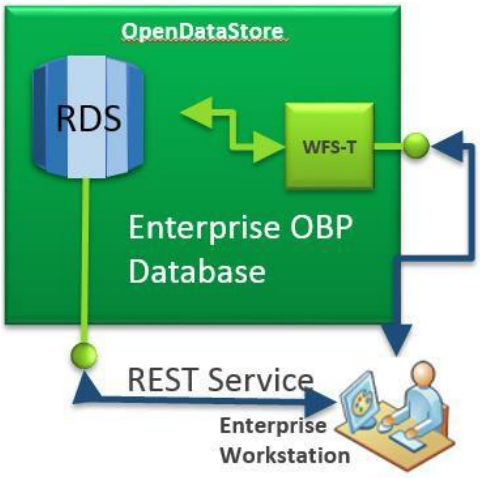
Aeronautical can do a two pronged approach. They lift and shift their current system to meet current cloud mandate.

At the same time, they develop their new capabilities in the cloud, using cloud native technologies. As soon as the new system is certified, they release the EC2/EBS instances used for the old system.

Eventual Target

The initial migration of NGA databases preserves the original schema and interfaces of the legacy Activities. Over time, the direct connect interfaces like the ODBC interfaces will be replaced with web based services and APIs, supporting looser coupling solutions and helping to enable methods such as Object Based Production (OBP). Once this is accomplished, and the data is abstracted from the activities, database consolidation can occur behind the scenes, as long as the published interfaces for the activities are maintained. Databases like the Aeronautical Safety of Navigation Database could be

consolidated into an overall Object Based Production database that would contain all NGS



feature/object data.

Figure I-0-7: Eventual Target Cloud Database

APPENDIX G-J: OPEN DATASTORE S3 BUCKET NAMING STANDARD (42 BUCKETS)

S3 Buckets Naming Standard			
Data Category	Government	Commercial	Host Nation
Geodesy	Geodesy-Government	Geodesy-Commercial	Geodesy-HostNation
Human Geography	HumanGeography-Government	HumanGeography-Commercial	HumanGeography-HostNation
Aeronautical	Aeronautical-Government	Aeronautical-Commercial	Aeronautical-HostNation
Maritime	Maritime-Government	Maritime-Commercial	Maritime-HostNation
Topographic Features	Topographic-Government	Topographic-Commercial	Topographic-HostNation
Targeting	Targeting-Government	Targeting-Commercial	Targeting-HostNation
Names & Boundaries	NamesBoundaries-Government	NamesBoundaries-Commercial	NamesBoundaries-HostNation
Controlled Imagery	ControlledImagery-Government	ControlledImagery-Commercial	ControlledImagery-HostNation
Elevation	Elevation-Government	Elevation-Commercial	Elevation-HostNation
Imagery	Imagery-Government	Imagery-Commercial	Imagery-HostNation
Intelligence Report	IntelligenceReport-Government	IntelligenceReport-Commercial	IntelligenceReport-HostNation
Knowledge	Knowledge-Government	Knowledge-Commercial	Knowledge-HostNation
Corporate	Corporate-Government	Corporate-Commercial	Corporate-HostNation
Unknown	Unknown-Government	Unknown-Commercial	Unknown-HostNation

S3 Bucket with Datasets mapped to it in the AR