

SECTION C - DESCRIPTION/SPECIFICATIONS/WORK STATEMENT

C.1 EXECUTIVE OVERVIEW

This contract defines the requirements for services supporting Foundation Cloud Hosting requirements, which align with the Department of the Interior’s (DOI) IT Transformation efforts.

The DOI’s IT Transformation efforts are designed to align with the “25-point Implementation Plan to Reform Federal IT”, the Federal Datacenter Consolidation Initiative (“FDCCI”), and the Cloud-First Policy outlined by the Federal Chief Information Officer (“CIO”). Federal IT Transformation efforts are designed to address two primary objectives:

1. Reduce the total cost of ownership of datacenter hosting hardware, software and operations; and
2. Provide greater service, security and support for application business owners and end-users.

The DOI’s goal is to establish the most, efficient, effective and transparent portfolio of IT service delivery solutions for meeting mission needs utilizing modern technology.

Initially, the DOI is seeking cloud-based services in the following six (6) technical service lines:

- Storage Services
- Secure File Transfer Services
- Virtual Machine Services
- Database Hosting Services
- Web Hosting Services
- Development and Test Environment Hosting Services

These technical service lines are intended to establish the initial infrastructure foundation for developing composite services that will be represented in a “Mission-Facing”, DOI-Wide IT Services Catalog.

Additionally, the DOI considers Data Center Consolidation or emergency operations requirements, and any hosting and associated support services necessary, to be within scope of this contract. Therefore, any modifications and/or task orders may be executed for any requirements within this area. This would include Contractor operation and maintenance of Government owned assets within either Government or Contractor owned and operated facilities.

C.2 OBJECTIVES

C.2.1 Business Objectives

The DOI’s business objectives for the IT Service Delivery program are as follows:

- a.** Improve availability, performance, and flexibility of datacenter services;
- b.** Reduce Total Cost of Ownership (“TCO”) of delivering IT services;
- c.** Promote the use of Green IT by reducing the overall energy, real estate footprint, and use of toxic components of DOI datacenters, and implementing effective recycling and reuse programs;
- d.** Ensure all applicable federal information security and privacy regulations are maintained and adhered to;
- e.** Provide tiered functions, service levels, and performance for customers;
- f.** Provide interoperable and portable solutions that enable mobility across hosting models and service providers; and
- g.** Enable scaling of infrastructure and application resources to meet evolving application and user demand.

C.2.2 Initial Technical Service Lines

The DOI is seeking cloud-based services in the following seven (7) technical service lines. These technical service lines are intended to establish the initial infrastructure foundation for developing composite services that will be represented in a “Mission-Facing”, DOI-Wide IT Services Catalog

C.2.2.1 Storage Services

The Storage Services Technical Service line includes, but is not limited to Cloud Based Storage Services in support of the DOI Continuity of Operations (CoOP), Disaster Recovery (DR), and Data Center Consolidation Transition Support Requirements.

C.2.2.2 Secure File Transfer Services

The Secure File Transfer Service Technical Service Line includes, but is not limited to an enterprise-wide capability for any employee, contractor or partner working on the DOI network to securely transfer files of any size and type to either internal or external business partners. This includes the capability for DOI employees, contractors and partners to receive files of any size and type from external business partners, while maintaining confidentiality and integrity, and the ability to manage the files in a web environment.

C.2.2.3 Virtual Machine Services

The Virtual Machine Services Technical Service Line includes, but is not limited to Cloud Based Virtual Machine Services in support of the Data Center Consolidation Transition Support and New Application Implementation Requirements. This Service Line may also be considered as an alternative to technical refresh of physical servers, a quick response resource to explore innovation opportunities, or rapid response multiprocessor multi-machine simulation environment.

C.2.2.4 Database Hosting Services

The Database Hosting Services Technical Service Line includes, but is not limited to, Cloud Based Database Hosting Services in support of the DOI Data Center Consolidation Transition and New Application Implementation Requirements. This service line may include stand-alone databases, shared data sources, or tiered database solutions including components of one or more other Technical Service Lines.

C.2.2.5 Web Hosting Services

The Web Hosting Services Technical Service Line includes, but is not limited to cloud Based Web Hosting Services in public, private, community and hybrid cloud environments. This service line may include any combination of other Technical Service lines necessary to deliver static and/or dynamic information to the DOI stakeholders, and includes hosting for an enterprise-wide content management system.

C.2.2.6 Development and Test Environment Hosting Services

The Development and Test Environment Hosting Service includes, but is not limited to providing a flexible, scalable, on-demand environment to support development, testing, staging, and/or quality assurance before releasing new applications and changes into the DOI production environment. They also support ad-hoc innovation activities. Change Control and User Permissions in this non-production environment are typically established on an instance by instance basis by the authorized user who provisioned the service.

C.3 INTRODUCTION TO TECHNICAL SERVICE DEFINITION MODEL

All technical services must fulfill a set of common, enterprise-wide requirements. Within each service line, technical services are defined based upon three dimensions: 1) Resource Requirements, 2) Service Level Requirements, and 3) Optional Characteristics Requirements. Additionally, each service line may require Associated Support Services to enable efficient migration from the current operating environment to the target operating environment, or to support sustained operations and maintenance of systems in the target operating environment. ***Figure 1 DOI IT Service Delivery Requirements*** below illustrates how these requirements and service dimensions fit together to define a Technical service.

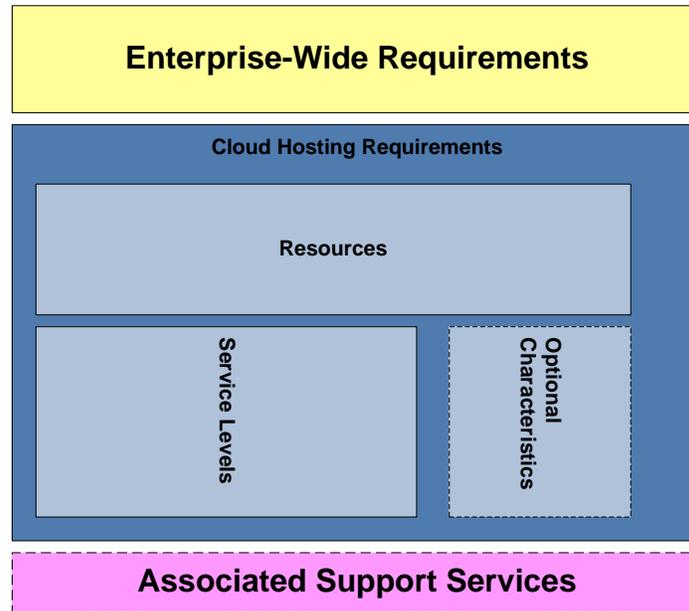


Figure 1 DOI IT Service Delivery Requirements

The Government shall retain ownership of any government designed/created/loaded data, policy, process, procedure, service template, workflow and application hosted on contractor’s infrastructure, and maintains the right to request full copies of these at any time.

C.3.1 Enterprise-Wide Requirements

Enterprise-Wide Requirements are baseline requirements common to all dimensions of the service definition, and are applicable to all service lines. Regardless of the resources, service levels, optional characteristics, or additional services selected to fulfill a specific service requirement, all Enterprise-Wide Requirements must be met. Enterprise-Wide requirements are described in Section C.5, Establish and Meet Enterprise-wide Requirements.

C.3.2 Resources Requirements

Resource requirements describe the platform, infrastructure assets, and support required by an information system to operate as defined by SLA’s and Operational Level Agreements (OLA’s). Examples of platform resource requirements include Operating Systems, Databases, and other Middleware used. Examples of infrastructure resource requirements include “Compute Host” and Storage. The Resources dimension is more completely described in Section C.6, Establish and Meet Resource Requirements.

C.3.3 Service Level Requirements

Service Level requirements define the performance and other operating parameters within which the hosting services must operate to fulfill IT system and customer requirements. The Service Level dimension is more completely described in Section C.7, Establish and Meet Portfolio of Service Level Requirements.

C.3.4 Optional Characteristics Requirements

Optional Characteristics define additional services that may be required by specific IT systems or hosting configurations that are not widespread enough to be considered a Resource or a Shared requirement. Examples of Optional Characteristics requirements include Forward Staging (including Content Delivery Networks and data application or telecommunications caching) and Operating System Patch Management. The Optional Characteristics dimension is more completely described in Section C.8, Optional Characteristics Requirements.

C.3.5 Associated Support Service Requirements

Associated support services are those services which may be required to enable identification, analysis, prioritization, preparation and migration of IT systems from the current operating environment to the target operating environment, or may be required to ensure sustained operations and maintenance of systems in the target operating environment. These Associated Support Services are more completely described in Section C.9, Associated Support Services.

C.3.6 Technical Service Definition Model Summary

The DOI objective is to design, procure and deliver technical services based upon the model described in this Section; therefore a “Technical Service” is defined as Resource or combination of Resources, provided at specified Service Levels, with specified Optional Characteristics, for a Fixed Price (FP) per unit of service. These Technical Services must be offered within the constraints of a common set of Enterprise-Wide requirements, and may require Associated Support Services. Individual Task Orders issued under this contract may define services and service lines through any combination of these service dimensions and/or technical service line definitions published in the DOI’s “Mission-Facing” Service Catalog.

C.3.7 Cloud Definitions and Basic Cloud Requirements

The DOI acknowledges that the cloud services market is still developing, and that there are a variety of approaches to defining cloud services. The DOI recognizes the cloud service definitions and deployment models specified in National Institute of Standards and Technology (NIST) 800-145, “The NIST Definition of Cloud Computing”. Service Models include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The Cloud deployment models consist of Public, Private, Community, and Hybrid.

[THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK]

Figure 2 NIST Cloud Computing Definition, below illustrates the NIST concept of Deployment Models, Essential Characteristics and Service Models for Cloud computing that the DOI has adopted.

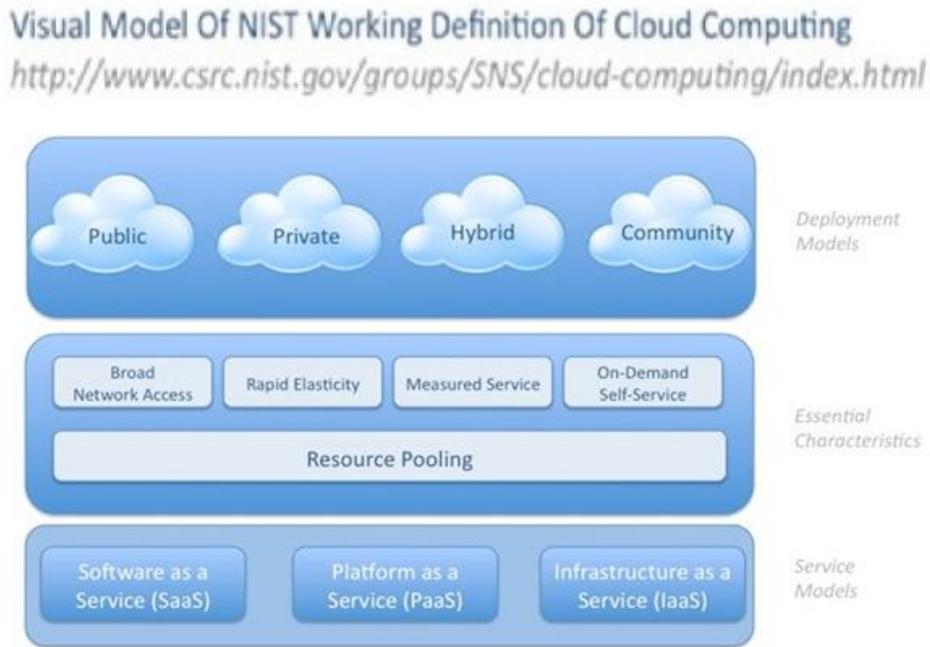


Figure 2 NIST Cloud Computing Definition

[THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK]

C.4 OVERVIEW OF CURRENT DOI OPERATING ENVIRONMENT

C.4.1 Organization

The U.S. Department of the Interior (DOI) is a Cabinet-level agency that manages America's vast natural and cultural resources. The DOI employs approximately 70,000 people, including expert scientists and resource-management professionals, in the nine technical bureaus, the federal shared service provider, and other supporting organizations listed below, herein after referred to as “Customer” organizations:

- Office of the Secretary (OS)
- Bureau of Indian Affairs (BIA)
- Bureau of Land Management (BLM)
- Bureau of Ocean Energy Management (BOEM)
- Bureau of Reclamation (BOR)
- Bureau of Safety and Environmental Enforcement (BSEE)
- National Business Center (NBC)
- National Park Service (NPS)
- Office of Surface Mining, Reclamation and Enforcement (OSM)
- U.S. Fish and Wildlife Service (FWS)
- U.S. Geological Survey (USGS)
- Other Interior Offices

There may be some organizational changes during execution of this contract, so the list above should not be considered definitive.

As part of the IT Transformation, the DOI is focused on an enterprise IT services model that will enable a unified strategy across the DOI and leverage a greater scale to drive more efficient operations.

C.4.2 Service Locations and End-points

DOI employees are located in over 2,400 offices in all 50 States, the District of Columbia, and U.S. Territories spanning 11 time zones. Approximately 80% of DOI employees work in locations with fewer than 25 total employees.

Many DOI employees and contractors regularly telework, travel or work for extended periods of time from remote field locations. Additionally, many DOI systems may need to be available to stakeholders in other government agencies and outside of the government domain.

C.4.3 IT Infrastructure Baseline

The DOI Bureaus and Offices currently deliver data and services from more than 400 locations. Over 30% of these locations and over 65% of DOI servers are located within one (1) hour driving distance of eight (8) metropolitan areas. The table below identifies key infrastructure metrics to support capacity analysis related to the current infrastructure.

Physical Servers	Storage Used (TB)	Racks	Gross Floor Area (sq. ft.)
~10k	>16k	>2,500	>300k

C.4.3.1 Data Centers

The DOI has applications and data distributed across over 400 datacenters, rooms, and closets throughout the United States.

Size (Gross Square Feet)	# Datacenters
<50	40
51-100	68
101-250	97
251-500	142
501-1,000	48
1,001 - 2,500	26
2,500- 5,000	16
>5,000	9

C.4.3.2 Data Center Access Channels

The DOI administers a Wide Area Network (WAN) that connects our internal customers, and provides the connection to external customers primarily via Trusted Internet Connection (TIC) sites. A number of remote sites may operate exclusively via dial-up circuits and satellite connections.

Additionally, the NBC, DOI's federal shared service center, currently provides virtual private networking services to more than 100 federal agency customers. These services are provided through Local Area Network (LAN), LAN-to-LAN Virtual Private Network (VPN) connectivity and Multi-Protocol Label Switching (MPLS)-dedicated circuits to both our hosting facilities and our Disaster Recovery (DR) sites.

Organizations within the DOI utilize a variety of WAN Optimization and application/desktop virtualization technologies to optimize utilization and available transport resources and meet end-user performance requirements.

C.4.3.3 Operating Systems

Operating System	% of Servers
Windows Server	63%
Unix Server	10%
Linux Server	17%
Other	10%

A more detailed description of operating systems in use can be found in Section C.6.1.1, Provide and Support Operating System Resource Requirements.

C.4.3.4 Enterprise Software Licenses

The DOI has a number of enterprise software licenses that are grouped into five (5) broad application classes:

1. Operating systems
2. Middleware (e.g., database managements systems)
3. Geographic Information System (GIS)
4. End-user productivity (e.g., collaboration)
5. Enterprise / mission applications (e.g., enterprise resource management, finance / HR, mission-specific)

A detailed description of the software in use is identified in 0 Establish and Meet Resources Requirements.

C.4.3.4.1 Categorization of Applications

The DOI's existing application environment presents a diverse set across a multitude of dimensions:

- a. **Type:** Enterprise applications (e.g., Finance/HR), public facing web sites/applications, mission-specific applications;
- b. **Software Source:** Commercial Off the Shelf (COTS), Government Off the Shelf (GOTS), DOI Custom, Aggregate Systems with DOI Developed Custom Interfaces.
- c. **Security Categories:** Applications span the full range of security FIPS Pub-199 security categories for confidentiality, integrity and availability impact: "LOW," "MODERATE," and "HIGH";
- d. **Hardware platform:** Applications cut primarily across Windows, Linux, and Unix, environments, with varying levels of modernization and customization;
- e. **Application environments:** Application code base include varying levels of legacy and modern programming languages and customization; and
- f. **Application Life-Cycle:** Steady State (Operations and Maintenance), Mixed State, and Development, Modification and Enhancement (DME).

C.4.3.4.2 Overview of Current Virtual Application Delivery Environment

The majority of applications reside upon corporate owned workstations. Several bureaus and offices within DOI have deployed existing Virtual Desktop and Application Delivery systems and a range of the solutions including but not limited to those listed below:

- Citrix XenDesktop
- Citrix XenApp
- VMWare View
- VMWare ThinApp
- Microsoft (Remote Desktop Services)
- Microsoft App-V

The existing systems are localized within the individual bureaus and are not scaled to support an enterprise the size of the DOI. There are approximately 30 significant instances of these technologies with an approximate combined concurrent license count around 5000.

The current DOI end user workstation environment consists primarily of Dell and IBM laptops/desktops running the Microsoft Windows XP or Windows 7 Operating System. However, there are also a growing number of mobile devices such as the Apple iPad/iPhone and Android/Windows Mobile tablet devices. While there is a wide range of desktop applications deployed, the applications common across the department consist of Microsoft Office Pro (2007/2010), Adobe, and select enterprise applications. The most common web browser is Internet Explorer, but others are also in use.

C.5 ESTABLISH AND MEET ENTERPRISE-WIDE REQUIREMENTS

Enterprise-Wide Requirements are baseline requirements that are common to all dimensions of the service definition, and are applicable to all service lines. Regardless of resources, service levels, optional characteristics, or additional services selected to fulfill a specific service requirement, all Enterprise-Wide Requirements must be met.

C.5.1 Comply with Essential Cloud Service Requirements

The Contractor shall provide a Cloud Computing solution that aligns to the following “Essential Cloud Service Characteristics” as defined in the NIST Working Definitions as described in **Table 1 Essential Cloud Services Characteristics** below:

Table 1 Essential Cloud Service Characteristics

Cloud Characteristic	Definition	General Requirement
C.5.1.1 On-demand self-service	A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.	The Contractor shall provide the capability for the ordering activity to unilaterally (i.e. without contractor review or approval) provision services.
C.5.1.2. Ubiquitous network access	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, laptops, and PDAs).	2a. The Contractor shall support internet bandwidth within minimum service requirements established herein. 2b. The Contractor shall have a minimum of two data center facilities at two different geographic locations in the Continental United States (CONUS), at least 250 miles apart, and all services acquired will be guaranteed to reside in CONUS, Alaska, Hawaii or US Territories.
C.5.1.3. Location independent resource pooling	The provider's computing resources are pooled to serve all consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The customer generally has no control or knowledge over the exact location of the provided resources 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, network bandwidth, and virtual machines.	The Contractor shall support scaling of resources based upon the minimum requirements described herein and specified within the individual Task Orders.
C.5.1.4. Rapid elasticity	Capabilities can be rapidly and elastically provisioned to quickly scale up and rapidly released to quickly scale down. To the consumer, the capabilities available for provisioning often appear to be infinite and can be purchased in any quantity at any time.	The Contractor shall support service provisioning and de-provisioning times (scale up/down), making the service available within minimum prescribed times of provisioning request.
C.5.1.5. Measured Service	Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.	The Contractor shall offer visibility into service usage via dashboard or similar electronic means.

C.5.2 Manage Service Delivery and Maintain Business Relationships and Interconnections

C.5.2.1 Provide Browser-based Management Functionality

The Contractor shall provide browser-based consoles, dashboards, portals, or interfaces for providing extensive self-service capabilities including (but not limited to):

C.5.2.1.1 Define User Roles and support User Authorization Workflows

Access to the Web management functionality shall be controlled via configurable role profiles that support highly customizable access rights including, but not limited to:

- A. Restricting access to each component of the console (e.g., restricting who can provision resources or view reports)
- B. Defining access rights for accessible components (e.g., scope of access, read-only versus read-write access)
- C. Administrator roles with the ability to create, modify, delete, and configure user accounts, profiles and permissions.
- D. Administrator capability to create authorization workflows with resource provisioning approval capabilities.

C.5.2.1.2 Provision, Configure, and De-provision (release) Resources

Access to the Web management functionality shall permit Provisioning, Configuring and De-provisioning resources and should include, but not be limited to the following:

- A. User-initiated provisioning of resources defined in Section C.6 “Resources”, as needed, without requiring human interaction with service provider; and
- B. Configuring automatic provisioning (where appropriate) as defined in Section C.7.1.2 “Demand Fluctuations”
- C. Resources (limit to templates identified in individual Task Orders)
- D. End-user devices (e.g., mobile devices such as smartphones)

C.5.2.1.3 Monitor Performance and Manage Alerts and Reporting

- A. General health and availability;
- B. SLA performance;
- C. Security;
- D. Resources;
- E. Configuring alarms and alerts; and
- F. Active Service Summary.

C.5.2.1.4 Monitor Resource Usage/Utilization and Provide Cost Metering/Controls

The general requirement under this section is to provide tools for ensuring that task order spending rates remain consistent with the funding levels and task durations. Additionally these tools should provide alerts as spending approaches 85% of contracted funding levels.

C.5.2.1.5 Manage Open and Resolved Incidents and Service Requests

The general requirement under this section is to provide integrated tools and context filtered reporting to enable transparent monitoring and reporting of government initiated, and government service impacting incidents and service requests. These management capabilities include, but are not limited to the following:

- Integrated system and subsystem status reporting and incident correlation to assess incident impact on multiple systems, services, programs and users, and to facilitate proactive communication with end-users, organizations and programs. This would include indicating both planned and unplanned downtime;
- On-line reporting of performance against key performance indicators identified in Section C.7 Establish and Meet Portfolio of Service Level Requirements, including, but not limited to: Mean Time to Resolve/Fix (MTF), Mean Time to Respond/Acknowledge (MTA);
- Prioritized queue of Incidents and Service Requests by Severity, with expected MTA and MTF based upon demonstrated performance. Including ability for authorized government official ability to establish/revise priorities and expedite;
- Repository of Reason for Outage (RFO) and Duration of Outage (DOO) information to support trend analysis and continual improvement efforts;
- Correlation of Complaints to Incidents;
- Rejected and Dropped Calls;
- Charting for Incidents per Hour, Day, Week, and/or Month over selected time period; and
- Integration with E-mail Alerts for incident volumes exceeding preset thresholds.

C.5.2.2 Support DOI System Interfaces

The Contractor shall provide the ability to connect a vendor-hosted system to another system that is hosted either at the DOI or at any external provider or customer, unless otherwise stated in specific Task Orders.

C.5.2.3 Implement Transparent and Effective Performance Management

The Contractor shall adhere to policies encouraging compliance with Service Level Agreements (“SLAs”) and other requirements (e.g., incentives, disincentives and Quality Assurance Plans).

The Contractor shall provide clear access and visibility to ongoing performance and resources usage including, but not limited to:

- a. Provide role filtered self management tools to support billing, monitoring, and reporting on service management functions;
- b. Provide visibility into usage metering using metrics and granularity appropriate to the type of service;
- c. Provide a suite of reports, dashboards, and alarms to monitor and track operational and infrastructure performance (e.g., incidents, service usage, capacity, SLA adherence);
- d. Provide automatic monitoring of resource utilization and other events such as failure of service, degraded service, etc. via service dashboard or other electronic means;
- e. Provide the ability to filter and view usage and invoicing by: Technical Service Line, bureau (and sub-bureau), program, IT System, IT System type, IT System Life-Cycle, Security Level, and other elements which may be identified in individual Task Orders;
- f. Provide access to all log files generated by the hosted application, associated middleware, operating system, and underlying virtual and physical infrastructure;
- g. Provide online reporting metrics interface for all resource utilization including metrics such as: current utilization, historical average and peak for a user defined window of time;

Additional performance management may be required by individual Task Orders. Reports shall be available for a period of time defined by the Task Orders.

C.5.2.4 Implement Efficient, Effective and Formal Governance

The Contractor shall specify policies and processes governing the interaction between the Contractor and the DOI, to include the following use cases:

- a. Incident Management;
- b. Process for monitoring and enforcing SLAs;
- c. Role-based Access and Provisioning Authorities and Workflows;
- d. Impact Plan in the event of a merger, acquisition, or divestiture;
- e. Process for adding, deleting, or changing requirements, technical service lines, service levels, resource templates and optional features;
- f. Process for assessing, planning, and mutual approval for achieving compliance with emerging regulations or policies.

C.5.2.5 Protect Intellectual Property Rights

The Contractor shall ensure the protection of DOI intellectual property (IP) and data ownership rights and those of any licensors.

C.5.2.6 Prohibit and Actively Prevent Adware, Spam, and Remarketing of Information

The Contractor shall not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the DOI. The Contractor and/or their agents shall not resell nor otherwise redistribute information gained from its access to the DOI.

C.5.3 Establish and Maintain Security and Privacy

C.5.3.1 Comply with FedRAMP and DOI Information Security and Privacy Requirements

The Contractor shall comply with the security and privacy requirements summarized in this section and as identified in the following Section J attachments:

- a.** Section J, Attachment 1 - DOI Security Control Standards;
- b.** Section J, Attachment 2 - Foundation Cloud Hosting Services Information Technology Security and Privacy Requirements for U.S. Department of the Interior;
- c.** Section J, Attachment 3 - DOI Privacy Loss Mitigation Strategy (PLMS); and
- d.** Section J, Attachment 4 - Additional IT Security Information;

The referenced attachments identify laws, rules, regulations, standards, technology limitations and other constraints that the Contract shall adhere to or work under.

The hosting environment provisioned by the service provider must demonstrate an appropriate level of security by meeting the requirements of the Federal Information Security and Management Act (FISMA) for moderate-impact systems, and related agency-specific policies. This includes a formal agency security authorization review covering security controls, continuous monitoring, and identification of risks. The agency must consider and accept the risks before Authority to Operate (ATO) will be granted. The service provider must qualify for ATO no later than 120 calendar days from the date of award. Moreover, the service provider must become compliant with Federal Risk and Authorization Management Program (FedRAMP) requirements within 120 calendar days of the date it becomes available, and must maintain compliance throughout the period of performance. The continuous monitoring provided must comply with the NIST Special Publication 800-137 framework and Department of Homeland Security (DHS) guidance.

C.5.3.2 Provide User Authentication and Secure Connections

The Contractor shall ensure seamless integration with the DOI Identity, Authorization and Access Management (IdAAM) solution enabling hosted systems to authenticate users as well as devices using those credentials without requiring additional solution credentials.

Range of authentication and secure connection solutions includes, but is not limited to:

- a.** Active Directory;
- b.** Lightweight Directory Access Protocol (LDAP);
- c.** Secure Socket Layer (SSL);
- d.** Secure Shell (SSH);
- e.** Kerberos;
- f.** RACF; and
- g.** HSPD-12/Token

C.5.3.3 Comply with Security Assurance Requirements

In addition to complying with the general security and privacy requirements referenced above, the Contractor shall develop a Security Assessment Plan and initially assess all applicable security controls, using an agreed upon independent third-party assessor, and provide security assessment results in a Security Assessment Report. The report shall include a characterization and articulation of known remaining risks in order to support the DOI Authorizing Official's (AO) Authority to operate (ATO). In accordance with the OMB memorandum entitled, Security Authorization of Information Systems in Cloud Computing Environments, issued on December 8, 2011, the DOI AO anticipates leveraging and accepting provisional authorizations granted by the FedRAMP Joint Authorization Board (JAB), to the extent available, in granting security authorizations and an accompanying authority to operate (ATO) for DOI use of the Contractor services. DOI does not necessarily anticipate leveraging authorizations granted independently by other individual agencies, but may opt to do so at its discretion.

C.5.3.4 Complete Third Party Assessment of Security Controls and Mitigate Weaknesses

Controls within the following security control families (as defined by NIST) must be assessed by a third party on behalf of the Contractor. Additionally, Contractors will be required to develop and implement a plan to mitigate any weaknesses related to these controls.

C.5.3.4.1 Implement and Maintain Access Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Access Control requirements listed in the Bidder's Security Questionnaire, Section J, Attachment 5 (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.2 Implement and Maintain Awareness and Training Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Awareness and Training requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.3 Implement and Maintain Audit and Accountability Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Audit and Accountability requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.4 Implement and Maintain Security Assessment and Authorization Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Security Assessment and Authorization requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements)

C.5.3.4.5 Implement and Maintain Configuration Management Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Configuration Management requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.6 Implement and Maintain Contingency Planning Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Contingency Planning requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.7 Implement and Maintain Identification and Authentication Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Identification and Authentication requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.8 Implement and Maintain Incident Response Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Incident Response requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.9 Implement and Maintain Maintenance Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Maintenance requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.10 Implement and Maintain Media Protection Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Media Protection requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.11 Implement and Maintain Physical and Environmental Protection Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Physical and Environmental requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.12 Implement and Maintain Planning Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Planning requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.13 Implement and Maintain Personnel Security Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Personnel Security requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.14 Implement and Maintain Risk Assessment Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Risk Assessment requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.15 Implement and Maintain System and Services Acquisition Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific System and Services Acquisition requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.16 Implement and Maintain System and Communications Protection Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific System and Communication Protection requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.17 Implement and Maintain System and Information Integrity Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific System and Information Integrity requirements listed in the attached Bidder's Security Questionnaire (which includes required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.4 Ensure Portability of IT Systems and Facilitate Migration between Service Providers

The Contractor shall ensure portability of IT Systems and facilitate migration of data and systems to another hosting solution (e.g., with another Contractor or within the DOI).

C.6 ESTABLISH AND MEET RESOURCE REQUIREMENTS

Resource requirements describe the platform, infrastructure assets, and support required by an information system to operate as defined by SLA’s and Operational Level Agreements (OLA’s).

Figure 3 Additional Detail on Resources and Service Levels below illustrates an example of how the resources and associated services align within the Cloud Service Models.

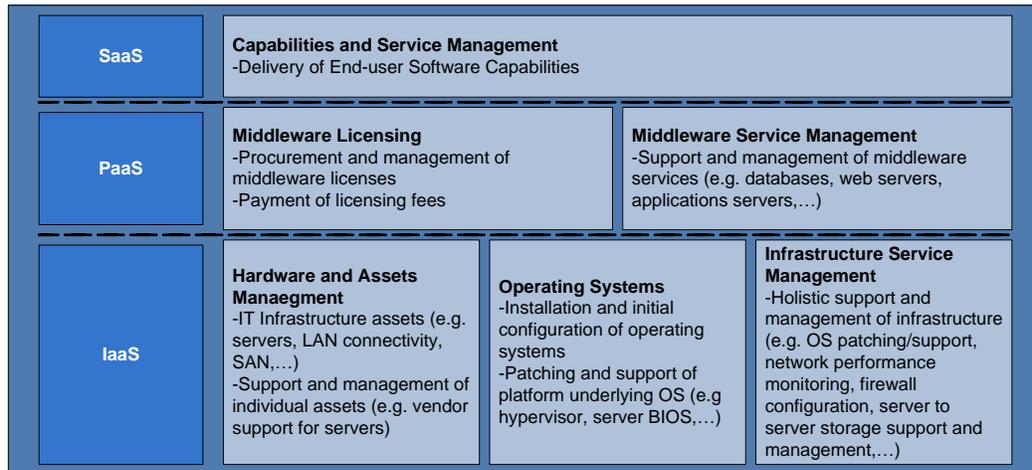


Figure 3 Additional Detail on Resources and Service Levels

Any requirements within this area will be specific in the individual Task Orders that may be required to address the resources outlined in this section along with the service level requirements addressed in Section.C.7, Establish and Meet Portfolio of Service Level Requirements.

C.6.1 Provide Basic Resources

C.6.1.1 Provide and Support Operating System Resource Requirements

The DOI operates an expansive set of operating systems across its various systems, which are outlined below. As described in the IaaS layer of Figure 4 Additional Detail on Resources and Service Levels, above, the DOI requires installation, configuration, patching, and support for the listed operating systems. There are several options for satisfying these requirements:

- a. The Contractor shall provide the required services for directly supporting these operating systems;
- b. The Contractor shall identify migration strategies and costs for transitioning to alternative operating systems, and provides the required services for the alternative operating system; and/or
- c. The Contractor shall provide only infrastructure, as described in the IaaS layer, and leave the operating system installation, configuration, patching, and support to the DOI.

Regardless of the services provided by a vendor, the Department retains the option to install, configure, patch, and support custom operating system images on top of vendor or Department-managed infrastructure.

The DOI requires a process for providing access and support for current requirements and new operating systems and versions as they become available and/or the Department's needs evolve. Additionally, the DOI may establish range of versions for each operating system which must remain available to support the base of hosted IT systems, including versions which may no longer be supported by the manufacturer.

The Contractor shall support current installed base of Operating Systems, which includes, but is not limited to:

- a. Windows Server: 2003 & 2008
- b. Linux: Centos 5.7, Red Hat 5, Red Hat 6, Ubuntu, SUSE Enterprise 10, Scientific
- c. Solaris 10 for SPARC
- d. AIX

The Contractor shall also support timely upgrade to current versions of the above Operating Systems.

C.6.1.2 Provide and Support Compute-Host Resources

Provide access to, and support for, compute host instances in a variety of performance levels defined in terms of compute power, RAM. The DOI has defined a "core" as the compute power equivalent to a 2 Ghz processor, unless otherwise specified in individual task orders.

[THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK]

In all options an equivalent solution of equal or better specifications will satisfy the requirement. The current installed base includes, but is not limited to those identified in Table 2 Minimum Compute-Host Configurations below:

Table 2 Minimum Compute-Host Configurations

Standard	Minimum Configurations	
	Cores (#)	RAM (GB)
Extra Small	1	2
Small	2	4
Medium	4	8
Large	8	16
Extra Large	16	16

High Memory

Extra Small	1	4
Small	2	8
Medium	4	16
Large	8	32
Extra Large	16	64

High Compute

Medium	4	2
Large	8	4
Extra Large	16	8

High Compute Cluster

Large	32	32
Extra Large	64	64

Custom

(Task Order Defined)	TBD	TBD
----------------------	-----	-----

C.6.1.3 Provide and Support Storage Resources

The Contractor shall provide the ability to provision storage services in a variety of performance classes, tiers, and/or pools. Performance classes shall be distinguished by the throughput supported by each class. The latency of storage accesses for all classes shall be in line with industry standards.

The service shall be available online, on-demand, and dynamically scalable up or down per request for service from the authorized users via Internet through a web browser.

All storage facilities that store Federal Records must meet NARA 1571 Archival Storage Standards (<http://www.archives.gov/foia/directives/nara1571.pdf>).

C.6.1.3.1 Identify and Provide Access to Storage APIs

The Contractor shall identify Application Programming Interfaces (APIs) required to access and manage storage.

C.6.1.3.2 Support Storage of Both Files and Data Objects

The Storage Services shall support storage of both files and storage of data objects.

C.6.1.3.3 Support Standard Storage Operations

The Storage Services shall support the operations identified in Table 3 Command/Request Definitions below.

Table 3 Command/Request Definitions

Request/Operation	Container/Bucket	Object/File
PUT	PUT operations performed against Container/Bucket are used to create that container.	PUT operations against an Object are used add object to the bucket/container and write, overwrite, an object's metadata and content.
GET	GET operations performed against Container/Bucket lists information about objects within that container/bucket.	GET operations against an Object are used to retrieve objects and the objects' data from the container/bucket.
HEAD	HEAD operations against a storage Container are used to determine the number of Objects, and the total bytes of all Objects stored in the Container.	HEAD operations against an Object are used to retrieve object's metadata and other HTTP headers.
DELETE	DELETE operations performed against Container/Bucket deletes the container/bucket.	DELETE operations against an Object are used to permanently delete the specified object.
POST POST is an alternate form of PUT that enables browser-based uploads	The POST request operation adds an object to a container/bucket using HTML forms.	POST operations against an Object name are used to set and overwrite arbitrary key/value metadata.
COPY	The COPY operation creates a new, uniquely named copy of a container/bucket that is already stored.	The COPY operation creates a uniquely name copy of an object/file that is already stored.
LIST	The LIST operation displays the information of a current Container/Bucket.	The LIST operation displays the current objects/files, including metadata.

C.6.1.3.4 Support Storage Resource Classes

For each Class proposed by the Offeror, a solution of equal or better specifications than identified in **Table 4 Proposed Storage Class** below will satisfy the requirement.

Table 4 Proposed Storage Class

Storage Class	Throughput	Uptime/ Availability	Example
A	8 Gbps	100%	high-speed SAN
B	1 Gbps	100%	low-speed SAN
C	50 Mbps	99.90%	Remote On-line Storage
D	Access within 24 hrs	offline	Tape Library

Independent Task Orders may specify selected storage class and availability requirements and may also specify that Class C and Class D storage be stored in a facility other than the one hosting the related mission system.

C.6.1.3.5 Support Data Migration Across Storage Classes

The Contractor shall provide support for migrating data across different classes. This support shall include a web-based interface for manually migrating data across different tiers as well as an open source API interface for accessing the same functionality.

C.6.1.3.6 Support Alternative Backup Solutions

The DOI requires the ability to design and manage backup solutions, and/or to utilize offeror-provided backup solutions.

The Contractor shall provide backup at both onsite and offsite locations, and may provide software solutions to manage the backup processes.

The Contractor shall ensure that all Archive and Backup services meet all of the requirements described in Section C.5.3, Establish and Maintain Security and Privacy.

The Contractor shall ensure the Web-management functionality includes:

- a. Ability to configure backup schedule;
- b. Ability to restore files and images from backup;
- c. Ability to configure a retention period and automatic deletions of old files;
- d. Ability for government to specify the level of redundancy required; and
- e. A scripting interface for the above.

C.6.1.3.7 Support Secure Transfer of Physical Media

When transferring physical media between locations, the Contractor shall provide a certified courier or other method of maintaining a secure chain of custody over tapes and other media being moved to and from a defined, secured off-site storage location. The Contractor shall provide flexibility in courier pick-up and delivery time.

C.6.1.4 Provide Transport Resources and Support Interconnections

C.6.1.4.1 Comply with General Transport Requirements

The DOI requires access to transport resources that meet the following requirements:

- a. The bandwidth consumed by each system shall be calculated using a 95th percentile method, with samples taken at a minimum of every five (5) minutes or less. The Contractor shall specify proposed range of sample rates within this range.
- b. Each system shall have access to sufficient bandwidth to meet its monthly data transfer needs as established in individual Task Orders.

C.6.1.4.2 Comply with Interconnection Configurations and Requirements

The Contractor shall support access to network connectivity in the following configurations:

- a. Between compute host instances;
- b. Between vendor datacenters;
- c. Between a vendor datacenter and the Department intranet;
- d. Between vendor datacenters and the internet; and
- e. Between vendor datacenters and DOI customers, including LAN-to-LAN VPN connectivity and dedicated circuits (e.g., T-1, DS-3, etc.).

C.6.2 Provide Aggregated Resources and Enabling Services

Aggregated Resource Services are combinations, or packages, of basic resources, (Operating System, Compute-Host, Storage, Telecommunications/Networking, Middleware, Scripting, and Programming).

Enabling Services describe reusable processes and activities that support multiple technical services. Additional Aggregated Resource Services and Enabling Services may be defined by the Contractor or by the DOI within individual Task Orders to facilitate communication, streamline ordering or provisioning, or simplify definition and pricing for higher order or advanced Services. Aggregated Resource Services and Enabling Services are high order components for defining Technical Services and Technical Service Lines delivered under the anticipated contract.

C.6.2.1 Provide Aggregated Resource Services

C.6.2.1.1 Provide Secure File Transfer Resources

The Contractor shall provide a Secure File Transfer solution that satisfies the requirements in Section J, Attachment 12, Secure File Transfer Requirements.

C.6.2.1.2 Provide Virtual Machine Resources

The service shall be available online, on-demand and dynamically scalable up or down per request for service from the end users via Internet through a web browser. **Table 5 Virtual Machine Service Requirements**, below provides a description of the general service and Resource requirements for Virtual Machines.

Table 5 Virtual Machine Service Requirements

Aggregate Resource Description	Resources
<p>Virtual Machines-</p> <ul style="list-style-type: none"> • Service shall provide scalable, redundant, dynamic computing capabilities or virtual machines. • Service shall allow Government users to procure and provision computing services or virtual machine instances online via the Internet. • Service shall allow users to remotely load applications and data onto the computing or virtual machine instance from the Internet. • Configuration and Management of the Virtual Machine shall be enabled via a Web browser over the Internet. 	<p>Compute-Host Resources</p> <p>CPU (Central Processing Unit) - CPU options shall be provided as follows:</p> <ul style="list-style-type: none"> • A minimum equivalent CPU processor speed of 2GHz shall be provided. Additional options for CPU Processor Speed may be provided, however it is not required. • The CPU shall support 32-bit or 64-bit operations . <p>RAM (Random Access Memory): Physical memory (RAM) reserved for virtual machine instance or Computing supporting a minimum of 1GB of RAM.</p> <p>Operating System (OS) Resources Service shall support at least the following OS: Windows, Unix, LINUX, or Solaris (Intel or SPARC).</p> <p>Storage Resources Disk Space options allocated for all virtual machines and file data supporting the minimum bundled storage.</p> <p>Transport Resources: Transport resources utilized to transfer data in/out of the provider’s infrastructure supporting the minimum data requirements.</p> <p>If there are costs associated with data transfer over and above ordinary transport charges, or there are special capabilities for bulk transfer, please indicate clearly in Section B pricing tables.</p>

Table 6 Virtual Machine Block Storage Service Requirements below provides a description of the general service and resource requirements for Virtual Machine Block Storage.

Table 6 Virtual Machine Block Storage Service Requirements

Service Description	Resources
<p>Disk/Block Storage Service –</p> <ul style="list-style-type: none"> • Service shall provide scalable, redundant, dynamic Web-based storage. • Service shall provide users with the ability to procure and provision block storage capabilities for cloud virtual machines remotely via the Internet. • Service shall provide block storage capabilities on-demand, dynamically scalable per request for virtual machine instances. 	<ul style="list-style-type: none"> • Block Storage –Once mounted, the block storage should appear to the virtual machine like any other disk.

The Government retains ownership of all virtual machines, templates, clones, and scripts/applications created with individual task orders issued under this contract as well as maintaining the right to request full copies of these virtual machines at any time.

The Government retains ownership of customer loaded software installed on virtual machines and any application or product that is developed under orders against this contract.

The Contractor shall:

1. Provide virtualization services for the customer to be able to spawn on-demand virtual server instances.
2. Support a secure administration interface, such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS) or Secure Shell (SSH), for the Government designated personnel to remotely administer their virtual instance.
3. Provide the capability to dynamically allocate virtual machines based on load, with no service interruption.
4. Provide the capability to copy or clone virtual machines for archiving, troubleshooting, and testing.
5. Provide multiple processor virtual machines.
6. Manage processor isolation in a multi-tenant environment.
7. Provide capability to perform live migrations (ability to move running VM's) from one host to another.
8. Provide a hypervisor which supports security features such as role-based access controls and auditing of administrative actions.
9. Provide a hypervisor which supports hardware-assisted memory virtualization.

C.6.2.1.3 Provide Database Hosting Resources

Specific Certification Requirements will be identified in the individual Task Orders. However, the following information should be considered a sampling of the current environment. Support Current Range of Database software, which includes, but is not limited to:

- a. Informix
- b. MS SQL Express
- c. MS SQL Server (2005, 2008, 2010, 2012)
- d. MySQL
- e. Oracle 10g
- f. Oracle 11g
- g. Oracle 8a
- h. PostGIS
- i. PostGreSQL
- j. SQLite
- k. Sybase IQ

The Contractor shall also support timely upgrade to current versions of the above database software.

The Contractor shall support additional database software as specified individual Task Orders.

C.6.2.1.4 Provide Web Hosting Resources

Specific Certification Requirements will be identified in the individual Task Orders. However, the following information should be considered a sampling of the current environment. Support Current range of Web Server software, which includes, but is not limited to:

- a. Apache
- b. TomCat
- c. Jeronimo
- d. IBM WebSphere
- e. ORACLE Application Server
- f. JRUN
- g. Glass Fish
- h. IBM HTTP Server
- i. IIS
- j. Jetty (Eclipse Foundation)

Contractor shall also support timely upgrade to current versions of the above Web Hosting Resources.

Contractor shall support additional Web Hosting Resources as specified in individual Task Orders.

C.6.2.1.5 Provide Development and Test Environment

The Contractor shall provide support for non-production environments with a range of instances of technical service lines. These non-production environments are characterized by different controls, boundaries and levels of access, which may be specified in the individual Task Orders.

C.6.2.1.6 Provide Application Hosting

Specific Certification Requirements will be identified in the individual Task Orders. However, the following information should be considered a sampling of the current environment. Support the current range of Application Server software, which includes, but is not limited to:

- a. Cold Fusion
- b. Glass Fish
- c. Hibernate
- d. JBOSSApp Server and Suite
- e. Matlab
- f. MediaWiki
- g. Oracle Application Server and BPM Middleware
- h. Silverlight
- i. Sun SMQ
- j. Tuxedo
- k. WebLogic
- l. WordPress

Contractor shall also support timely upgrade to current versions of the above Applications. Contractor shall support additional Applications as specified in individual Task Orders.

C.6.2.2 Provide Enabling Services

C.6.2.2.1 Support Bulk Data Transfer and Provide Competitive Volume Discounts

The Contractor shall provide volume pricing, for periodically transferring large amounts of data into or out of the Contractor-hosted environment, and between sites within the Contractor environment. These transfers may originate or terminate at both DOI and non-DOI facilities (e.g., universities). The volume of data transferred could range from the size of virtual machine images to all of the DOI data stored in the Contractor environment.

The Contractor shall support the following modes for Bulk Data Transfer:

- a. Loading data from physical media (e.g., disk arrays, tapes, DVDs)
- b. Transferring data in/out over the Internet
- c. Transferring data in/out to the DOI intranet
- d. Transferring data in/out via dedicated circuits (including virtual private networks).

C.6.2.2.2 Provide Operating System Services

The DOI requires several operating system services. All services can be performed by either the Contractor or the DOI, but the DOI retains the right to perform any service itself. These services include configuring Operating Systems and troubleshooting Operating System Problems.

C.6.2.2.3 Provide Licensing and Installation Services

The DOI requires the licensing and installation of all necessary operating systems and software that is the Contractor responsibility under service or service line bundles.

C.6.2.2.4 Provide Patching and Version Control Services

The Contractor must commit to a defined patching schedule and process (e.g., the DOI shall be notified in advance and given sufficient time to test compatibility with all related software – example time for implementation could range from a few days to a few weeks after identification).

The Contractor shall comply with negotiated change control processes and authorities for change, as mutually agreed upon after award. The Contractor shall coordinate with the system owner prior to making changes to the hardware configuration that may also require changes to the business system.

All proposed modifications shall be documented, tested, planned and communicated to client to ensure compatibility with the business system and to include fall back procedures. The Contractor shall provide the DOI at least one (1) week to test patches before they are rolled out to production systems. The DOI may postpone the patch indefinitely for selected environments if it is unable to make deployed IT systems compatible with the new versions.

The Contractor shall cooperate with the DOI to establish recurring maintenance windows and limit all but critical security patches to distribution within these windows.

C.6.2.2.5 Provide Disaster Recovery Services

For all Disaster Recovery the Contractor shall provide the following services:

- A.** Support to design, implement, and manage the Disaster Recovery solution
- B.** Provide a web-based capability for configuring Disaster Recovery options.
 - I.** Establish a set of mission critical data and snapshots.
 - II.** Provide all services required in order to execute failover in the event of disaster and bring mission critical systems and data online.

C.6.2.2.6 Support One or More Solutions for Middleware Licensing and Support

The DOI operates an expansive set of middleware platforms across its various systems, which support Web Hosting, GIS, Database and Applications. The DOI requires licensing and management services for all middleware platforms identified herein. There are several options for satisfying these requirements:

- A. Contractor Provided Licensing and Management for Current Portfolio.** The contractor shall provide the licensing and/or management services for directly supporting current portfolio of DOI platforms and additional platforms as may be identified in individual Task Orders; and/or
- B. Contractor Proposed Migration to Recommended Standard.** The Contractor shall identify migration strategies and costs for transitioning to an alternative platform, and provides the licensing and/or management services for the alternative platform; and/or
- C. DOI Provides Licensing and Management.** The Contractor shall provide only infrastructure, as described in the IaaS layer, and DOI shall manage and license middleware.

Regardless of the services provided, the DOI retains the option to install, manage, and provide its own support for middleware instances on top of Contractor or DOI-managed infrastructure.

C.6.2.2.7 Provide Hosting for DOI Legacy Metering and Reporting Software. However, the following information should be considered a sampling of the current environment. Support the current range of Metering and Reporting software, which includes, but is not limited to:

- a.** Actuate
- b.** AWStats
- c.** Crystal Reports
- d.** Fiddler
- e.** Groundworks
- f.** Hyperion SQR
- g.** IBM Applications Service Center
- h.** Jasper Server
- i.** MS SCOM
- j.** NAGIOS
- k.** SmarterStats
- l.** Splunk
- m.** Windows Log Parser

Contractor shall also support timely upgrade to current versions of the above legacy metering and reporting software. Contractor shall support additional metering and reporting software as specified in individual Task Orders.

C.6.2.2.8 Provide Hosting for Other Middleware

Specific Certification Requirements will be identified in the individual Task Orders. However, the following information should be considered a sampling of the current environment. Support the current range of Other Middleware, which includes, but is not limited to:

- a. Atlassian JIRA
- b. Adobe Pro
- c. ArborText
- d. Citrix XenApp
- e. Citrix XenDesktop
- f. Citrix XenServer
- g. Common Spot
- h. CommVault
- i. Documentum
- j. Exlips Plut-ins
- k. Entellitrak
- l. Hydra
- m. IBM FileNet
- n. Microsoft Dynamix CRM 2011
- o. Net Backup
- p. Networker
- q. Oracle ADF
- r. Prolifics
- s. PureDisk
- t. SharePoint
- u. Software AG/Entirex DCOM (Communicator, XML Mediator, Adapters)
- v. SQL Forms
- w. Web Center Content
- x. XML Data Powers

Contractor shall also support timely upgrade to current versions of the above Middleware. Contractor shall support additional Middleware as specified in individual Task Orders.

C.6.2.2.9 Provide Hosting for Scripting and Programming Environments

The DOI requires access to the following scripting languages on all web and application servers.

- a. .NET
- b. ASP.net
- c. Flex Action Script
- d. ISAPI
- e. Java
- f. Java Script
- g. Jscript
- h. Node.js
- i. 4GL
- j. Perl

- k. PHP
- l. Python
- m. RScript
- n. Ruby on Rails
- o. UNIX Scripting

Contractor shall also support timely upgrade to current versions of the above scripting and programming environments. Contractor shall support additional scripting and programming environments as specified in individual Task Orders.

C.6.2.2.10 Provide or Support Virtual Application and Virtual Desktop Resources

A. Support Virtual Application/Desktop Capabilities-

The DOI desires to meet the following Application/Desktop Virtualization Goals:

- The ability for our users to leverage any device, anywhere, at any time, with the appropriate level of information assurance.
- The ability to equip users quickly with necessary tools, improve customer service, and lower costs.
- An enterprise-class virtual desktop/application solution that may scale to service all government employees within the scope of the task order award.

B. Support General Virtual Application/Desktop Capabilities

Table 7 Virtual Application and Desktop User Needs below, identifies a representative list of DOI user requirements for virtual applications and desktops.

Table 7 Virtual Application and Desktop User Needs

User Needs
The ability to work from home and on “Personally Owned Equipment” (POE), even when using computationally intensive tasks.
The ability to work in other DOI facilities and Federal, State and Local Partners (public, private and non-profit).
The ability to share large amounts of data with external partners at their locations.
The ability to collect information while in field locations with no connectivity and upload the information without having to come into the office (via from home or other locations with cellular, WI-FI, or wired connection to the Internet).
The ability to collect and analyze data while in the field or on travel, accomplish office work, and use the same device for possible non-business purposes due to weight or space restrictions.
The ability for remote access to DOI information using mobile devices without smart card readers
The ability for authorized government users to specify custom desktop images which include a wide range of applications, and deploy these images within timelines which may be identified in the individual task orders.
The ability to conduct self-service password reset from outside the network.

C. Support Additional Virtual Application/Virtual Desktop Requirements

Virtual Application and Virtual Desktop solutions should satisfy user requirements, use cases and other requirements identified in the individual task orders.

C.7 ESTABLISH AND MEET PORTFOLIO OF SERVICE LEVEL REQUIREMENTS

Service Level requirements define the performance and other operating parameters within which the infrastructure must operate to meet IT System and End User requirements. For this section "Days" refer to calendar days unless an alternative definition is explicitly provided for a specific service level metric in individual task orders.

C.7.1 Optimize End-to-End Performance

C.7.1.1 Manage Latency between Hosted Applications and End Users

Latency shall be managed, by the Contractor, so as to optimize IT System responsiveness to end users and ensure functionality of the hosted application. The Contractor shall cooperate with the DOI to configure and maintain system infrastructure elements to ensure end-to-end latency is in compliance with IT system and end-user service level commitments. The assumption of both parties during the evaluation and resolution of end-to-end latency issues shall be that there is joint responsibility, and only upon identification of the latency issue(s) shall final responsibility be assigned. Additionally, the Contractor shall provide or cooperate with the DOI to deploy Virtual Application Hosting to improve user experience. Specific latency requirements, if any, will be identified in individual task orders.

C.7.1.2 Adapt to Demand Fluctuations to Meet and Maintain Service Levels

The Contractor shall ensure that system infrastructure is able to accommodate fluctuations in demand with minimal impact on system performance. Anticipated seasonality, minimum, peak and average demand rates will be provided in individual task orders to facilitate resource planning. Individual Task Orders may identify selected methods and minimum times for adapting to demand fluctuations.

C.7.1.3 Streamline and/or Automate Resource Scaling

The Contractor shall provide several tiers of service for the scale of basic resources that must be readily provisionable at all times. The Contractor shall provide capability to template incremental tiers for each resource or service package. Alternative methods for meeting the objective to streamline incremental provisioning for common, cost effective configurations based upon appropriate combinations to scale based upon application Input-Output (I/O), Processor, Memory or Storage sensitivity will also be considered. The DOI approved tiers/templates shall be selectable within the provisioning portal, and authorized users shall be able to establish the resource scaling sequence most appropriate to their application when configuring automatic scaling. Minimum timelines for implementing scaling options may be identified in individual Task Orders.

C.7.2 Meet Software and Licensing Support Service Level Requirements

C.7.2.1 Meet Operating System Services Service Level Requirements

Specific Service Levels for Operating Systems may be identified in the individual Task Orders.

C.7.2.2 Meet Licensing and Installation Services Service Level Requirements.

Specific Service Levels for Licensing and Installation may be identified in the individual Task Orders.

C.7.2.3 Meet Patching and Version Control Services Service Level Requirements.

Specific Patching and Version Control Service Levels may be identified in the individual task orders.

C.7.3 Meet Uptime and Availability Requirements

The Contractor shall guarantee several tiers of uptime of all Contractor controlled resources in terms of percentage of minutes a month that the Contractor controlled resources shall be fully operational and available. Planned downtime, as defined in **Table 17 Scheduled Downtime Service Bands**, Meet Mean-Time-To- Restore Service Levels, is counted as the system being fully operational. **Table 8 Uptime and Availability Service Bands** below identifies the minimum performance levels required for uptime and proposes options for up to four (4) service bands. The Contractor shall meet the minimum performance requirement, but may propose one (1) to four (4) alternative service bands.

Table 8 Uptime and Availability Service Bands

Uptime			
Service Band	Minimum (>=)	Maximum (<)	Maximum Planned Downtime
Band 1	99.99%	100%	<4 min/month
Band 2	99.90%	99.99%	<43 min/month
Band 3	99%	99.90%	<7.2 hours/month
Band 4	95%	99%	<36 hours/month
Minimum Acceptable Performance:	95%		<36 hours/month

C.7.4 Meet Disaster Recovery Services Service Levels

The DOI requires a Disaster Recovery plan that meets all requirements outlined herein, and Recovery Time Objective (RTO) and Recovery Point Objective (RPO) specified below and in the individual task orders. Additional, Specific Disaster Recovery Service levels may be identified in the individual task orders.

C.7.4.1 Meet Recovery Time Objectives (RTO)

The Contractor shall guarantee that, following any outage attributable to failure of the infrastructure support, systems will be made operational within a specified maximum time. The table below identifies the minimum performance level for RTO and proposes options for up to five (5) service bands. The Contractor shall meet the minimum performance requirement, but may propose one (1) to five (5) alternative service bands.

Table 9 Recovery Time Objective Service Band Recommendations

Recovery Time Objective (RTO)		
Service Band	From	To
Band 1	0 minutes	5 minutes
Band 2	5 minutes	4 hours
Band 3	4 hours	24 hours
Band 4	24 hours	48 hours
Band 5	48 Hours	7 Days
Minimum Acceptable Performance:		7 Days

C.7.4.2 Meet Recovery Point Objectives (RPO)

The Contractor shall guarantee that, following a triggering event, systems will be reverted to a prior state no older than the specified maximum duration. Table 10 Recover Point Objectives below identifies the minimum performance level for RPO and proposes options for up to five (5) service bands. The Contractor shall meet the minimum performance requirement, but may propose one (1) to five (5) alternative service bands.

Table 10 Recover Point Objectives

Recovery Point Objective (RPO)		
Service Band	From	To
Band 1	0 minutes	5 minutes
Band 2	5 minutes	4 hours
Band 3	4 hours	24 hours
Band 4	24 hours	48 hours
Band 5	48 Hours	7 Days
Minimum Acceptable Performance:		7 Days

[THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK]

C.7.5 Meet Backup Service Levels

The following service level requirements apply to Backup Services.

C.7.5.1 Comply with Backup Frequency Requirements

The Contractor shall provide a means of configuring backup and archiving frequency on an authorized technical user defined schedule. The schedule shall support daily, weekly, monthly, and yearly backups. The DOI authorized technical user shall be able to select a different Mean Time to Restore and Retention Periods for each backup. Specific Backup Frequency requirements may be identified in the individual Task Orders.

An example backup schedule could be:

Table 11 Recommended Backup Service Levels and Retention Periods

Backup Service Levels		
Frequency	Retention Period	Mean-Time to Restore
Daily	2 weeks	15 minutes
Weekly	1 month	4 hours
Monthly	1 year	24 hours
Yearly	48 Hours	72 hours

C.7.5.2 Meet Mean Time to Restore Requirements.

The average time required to complete a restore request. Given that the size of a restore request will influence time required to restore it, these service levels are calculated as the average of all restore requests (both big and small) over a month. Specific Mean-Time to Restore requirements may be identified in the individual Task Orders.

Table 12 Mean Time to Restore Requirements

Backup Service Levels	
Service Band	Mean-Time to Restore
Band 1	15 minutes
Band 2	4 hours
Band 3	24 hours
Band 4	72 hours

C.7.5.3 Comply with Data Retention Policies

The retention period is the duration that each backup snapshot will be retained before automatic deletion. The DOI requires the ability to set a custom time period within individual Task Orders.

C.7.6 Document and Meet Provisioning Service Level Requirements

The Contractor shall provide several tiers of service for the speed in which a hosted system can respond to changes in demand. In all cases resources shall be brought online and available for use within the specified time as defined within the individual task orders.

For example, in order to retain flexibility to scale up resources quickly to respond to sudden spikes in demand, some systems may subscribe to a top tier. Other systems, though, with more predictable changes in demand may be able to plan further ahead and subscribe to lower tiers of service.

After a request has been made (either manually or automatically in response to configurable triggers), resources (e.g., storage, virtual machines) shall be available for use within the specified times.

C.7.6.1 Meet Compute Host and Operations System Provisioning Service Level Requirements

The Contractor shall provide a means to provision the Compute Host manually, and/or scale Compute Host Resources both manually and automatically. The Table 13 Compute Host Service Bands below identifies the minimum performance level and proposes options for up to four (4) service bands. The Contractor shall meet the minimum performance requirement, but may propose one (1) to four (4) alternative service bands. Time measurement assumes that the user possess appropriate provisioning authorization credentials.

Table 13 Compute Host Service Bands

Service Band	Minimum (\geq)	Maximum ($<$)
Band 1	0 min	15 min
Band 2	15 min	2 hours
Band 3	2 hours	8 hours
Band 4	8 hours	24 hours
Minimum Acceptable Performance:		24 hours

C.7.6.2 Meet Storage Provisioning Service Level Requirements

The Contractor shall provide a means to provision the Storage both manually, and/or scale Storage Resources both manually and automatically. The table below identifies the minimum performance level and proposes options for up to four (4) service bands. The Contractor shall meet the minimum performance requirement, but may propose one (1) to four (4) alternative service bands. Time measurement assumes that the user possess appropriate provisioning authorization credentials. Table 14 Storage Provisioning Service Bands identifies proposed Service Bands for Provisioning Storage.

Table 14 Storage Provisioning Service Bands

Service Band	Minimum (>=)	Maximum (<)
Band 1	0 min	15 min
Band 2	15 min	2 hours
Band 3	2 hours	8 hours
Band 4	8 hours	24 hours
Minimum Acceptable Performance:		24 hours

C.7.7 Meet Middleware Management Service Level Requirements

The Contractor shall provide several tiers of management support for Database, Web Server, and Application Servers. These services shall include the following requirements:

C.7.7.1 Meet Middleware Patching and Version Control Requirements

The Contractor shall commit to a defined patching schedule and process (e.g., the DOI must be notified in advance and given sufficient time to test compatibility with all related software – example time could range from a few days to a few weeks, and could postpone the patch indefinitely if it could not be made compatible). This section also defines any requirements around how quickly the Contractor shall make new versions of any support software available for use.

The Contractor shall provide the DOI test patches at least 1 week before they are rolled out to production systems.

The Contractor shall ensure all proposed modifications are documented, tested, planned and communicated to consumer to ensure compatibility with the business system and to include fall back procedures.

The Contractor shall coordinate with the system owner prior to making changes to the hardware configuration that may also require changes to the business system.

Required Schedules:

- a. Weekly
- b. Monthly
- c. Quarterly
- d. Yearly

C.7.7.2 Meet Additional Middleware Service Level Requirements

The Contractor shall meet additional middleware service level requirements which may be identified in the individual Task Orders.

C.7.8 Meet Secure File Transfer Service Levels

Specific service level requirements for the Secure File Transfer technical service line will be identified in the individual task orders. Section J, Attachment 12 identifies the initial requirements for this technical service.

C.7.9 Meet Virtual Desktop and Applications Service Levels

Specific service level requirements for Virtual Desktop and Applications Services will be identified in the individual Task Orders.

C.7.10 Meet Customer and Program Support Service Levels

The DOI requires several tiers of support for any support services provided. Support services include both trouble ticket support, as well as service management (e.g., Infrastructure Service Management, Operating System Service Management, and Middleware Service Management).

For each tier of support, the DOI requires pre-defined service levels for the following metrics:

- a. Availability (defined in section C.7.11.1 Meet Service Center Availability Service Levels)
- b. Time to Respond (defined in section C.7.11.2 Meet Service Level Time To Respond (Acknowledge) to Requests Service Levels)
- c. Time to Resolve (defined in section C.7.11.3 Meet mean-time-to-resolve service levels)
- d. Planned downtime (defined in Table 19 in Section c.7.11.4 Minimize Planned Downtime in Maintenance Windows)

The DOI requires the following definition of support and service request severity:

- a. Severity 1: Emergency (Health and Safety)
- b. Severity 2: Mission Priority (Bureau Director)
- c. Severity 3: Program Priority
- d. Severity 4: Routine

In addition, within thirty (30) calendar days of any major outage occurrence resulting in greater than 1-hour of unscheduled downtime, the Contractor shall describe the outage including description of root-cause and fix.

C.7.10.1 Meet Service Center Availability Service Levels

During hours of availability the customer expects to reach a support or service person who is able to take down a request for service or log a trouble ticket. Specific Service Center Availability Service Levels will be selected from the available tiers in the individual task orders.

- e. Meet Mean-Time-To-Resolve Service Levels)
- f. Planned downtime (defined in Table 19 in section C.7.11.4 Minimize Planned Downtime and Maintenance Windows)

The DOI requires the following definition of support and service request severity:

- e. Severity 1: Emergency (Health and Safety)
- f. Severity 2: Mission Priority (Bureau Director)
- g. Severity 3: Program Priority
- h. Severity 4: Routine

In addition, within thirty (30) calendar days of any major outage occurrence resulting in greater than 1-hour of unscheduled downtime, the Contractor shall describe the outage including description of root-cause and fix.

C.7.10.2 Meet Service Center Availability Service Levels

During hours of availability the customer expects to reach a support or service person who is able to take down a request for service or log a trouble ticket. Specific Service Center Availability Service Levels will be selected from the available tiers in the individual task orders.

The DOI requires the following tiers of availability:

C.7.10.2.1 8x5 Single Time zone

- 9am to 5pm
- Monday through Friday
- in a single time zone which may be identified in the individual task orders

C.7.10.2.2 8x5 CONUS

- 9am to 5pm
- Monday through Friday
- in each of the 4 CONUS Time zones (Eastern, Central, Mountain, and Pacific)

C.7.10.2.3 8x5 CONUS + Alaska

- 9am to 5pm
- Monday through Friday
- in each of the 4 CONUS Time zones (Eastern, Central, Mountain, and Pacific) plus Alaska

C.7.10.2.4 24x7x365/366

- 24 hours a day
- 7 days a week

C.7.10.2.5 Custom Work Hours, Custom Work Week, Selected Time Zone(s)

- To be defined in individual Task Orders.

C.7.10.2.6 Defined Season or Emergency/Incident Support

- To be defined in individual Task Orders.

C.7.10.3 Meet Service Level Time To Respond (Acknowledge) to Requests Service Levels

After contacting support, the DOI requires an acknowledgement of the request and initial service center within the specified time to respond.

Table 15 Service Levels for Acknowledging Requests below identifies the tiers of service required by the DOI. Severity/Priority levels in Section C.7.10, Meet Customer and Program Support Service Levels.

Table 15 Service Levels for Acknowledging Requests

	Severity/Priority							
	1		2		3		4	
Service Band	Minimum (>=)	Maximum (<)	Minimum (>=)	Maximum (<)	Minimum (>=)	Maximum (<)	Minimum (>=)	Maximum (<)
Band 1	0 min	15 min	0 min	30 min	0 min	45 min	0 min	60 min
Band 2	15 min	2 hr	30 min	4 hr	45 min	6 hr	60 min	8 hr
Band 3	2 hr	8 hr	4 hr	16 hr	6 hr	24 hr	8 hr	36 hr
Band 4	8 hr	24 hr	16 hr	48 hr	24 hr	72 hr	36 hr	96 hr

C.7.10.4 Meet Mean-Time-To-Resolve Service Levels

The DOI requires a commitment on the mean time to resolve all service and support issues. Time is calculated from initial response until satisfactory resolution or escalation. Averages are calculated monthly.

Table 16 Service Levels for Mean-Time-To Resolve (Fix) below identifies the DOI required service bands, Severity/Priority levels in Section C.7.10, Meet Customer and Program Support Service Levels.

Table 16 Service Levels for Mean-Time-To Resolve

	Severity/Priority							
	1		2		3		4	
Service Band	Minimum (>=)	Maximum (<)	Minimum (>=)	Maximum (<)	Minimum (>=)	Maximum (<)	Minimum (>=)	Maximum (<)
Band 1	0 min	15 min	0 min	30 min	0 min	45 min	0 min	60 min
Band 2	15 min	2 hr	30 min	4 hr	45 min	6 hr	60 min	8 hr
Band 3	2 hr	8 hr	4 hr	16 hr	6 hr	24 hr	8 hr	36 hr
Band 4	8 hr	24 hr	16 hr	48 hr	24 hr	72 hr	36 hr	96 hr

C.7.10.5 Minimize Planned Downtime and Maintenance Windows

The Contractor shall provide support services that accommodate several maintenance window maximums. Planned downtime must occur at times specified in the individual task orders, and agreed upon with each application system owner. Proposed Service Bands for Scheduled Downtime are identified in Table 17 Scheduled Downtime Service Bands.

Table 17 Scheduled Downtime Service Bands

Service Band	Maximum Scheduled Downtime Per week	
	Minimum (>=)	Maximum (<)
Band 1 (High Availability)		0.1 min
Band 2	0.1 min	1 hr
Band 3	1 hr	2 hr
Band 4	2 hr	4 hr
Band 5	4 hr	8 hr

C.8 OPTIONAL CHARACTERISTICS REQUIREMENTS

Optional Characteristics Requirements define additional services that some systems require, but are not widespread enough to be considered a Resource or a Shared requirement.

C.8.1 Support Resource Segregation Options

The Contractor shall provide several options for segregating DOI resources:

- a. Fully segregated – DOI hosted systems (physical and virtual) must not share resources with any non-DOI entities. The Contractor shall provide physical barriers to separate customer’s equipment.
- b. Federal government segregation – DOI hosted systems (physical and virtual) must not share resources with any non-Federal Government entities. The Contractor shall provide physical barriers to separate Federal government equipment from non-Federal government equipment.
- c. Non-segregated – DOI hosted systems (physical and virtual) can share resources with other entities.

Specific requirements for Resource Segregation may be identified in the individual Task Orders.

C.8.2 Support Non-production environments

The Contractor shall provide the ability to define non-production environments (e.g., test, development, training, staging, sandbox) as customized copies of a production environment. A non-production environment shall default to the same Resources, Service Level, and Feature requirements as the production environment, and a DOI administrator shall have the ability to adjust the non-production environment specifications.

Non-production environments may need access to Production storage or middleware instances, or may require separate clean storage and middleware instances. Non-production environments may require a means of populating storage from sources, both inside or outside, of the Contractor environment. The Contractor shall provide the ability to restrict access to non-production environments to a different set of users or “domains”. For example, in relation to a Production environment a Development environment may have:

- a. Same middleware and operating system Resource requirements
- b. Lower Compute Host, Storage, and Bandwidth Resource requirements
- c. Lower Service Level requirements
- d. An option of Persistent or Non-persistent storage

The DOI shall have the ability to create and destroy non-production environments via web console.

Specific requirements Non-Production Environments may be identified in the individual Task Orders.

C.8.3 Support Requirement to Manage Underlying Physical Resources

The Contractor shall provide the functionality to manage the infrastructures underlying physical resources. For example, for licensing reasons, some systems need to attach a particular VM to a process and prevent it from being reassigned.

Specific requirements for Management of Underlying Physical Resources may be identified in the individual Task Orders.

C.8.4 Provide Content Delivery Network (CDN)

The Contractor shall provide the ability to cache static content at locations around the US to provide fast access to local users. This functionality is also known as Forward Staging.

Specific requirements for CDN may be identified in the individual Task Orders.

C.8.5 Support Government Compliance Requirements

The Contractor shall comply with government security and regulatory requirements that systems are subject to beyond those that the entire DOI is subject to. These regulations may include, but are not limited to:

- a. Ability to provide forensics on the roaming profiles of virtual desktop users
- b. Adherence to International Traffic in Arms Regulations (ITAR) requirements
- c. Adherence to Electronic Code of Federal Regulations (e-CFR) 250 regulations and Outer Continental Shelf (OCS) Lands Act
- d. Adherence to any restrictions placed on proprietary data stored by the Department
- e. Adherence to any litigation hold requirements currently in place or that may be imposed in the future
- f. Adherence to security controls defined in Section J, Attachment 1, DOI Security Control Standards

Government Compliance requirements may be identified in the individual Task Orders.

C.8.6 Support Alaska/Hawaii Regional Connectivity

The Contractor shall ensure users in Alaska and Hawaii can access core systems and data even when connectivity to CONUS has been lost. Definition of “core systems and data” must be configurable on a per application basis. Specific requirements for Regional Connectivity may be identified in the individual Task Orders.

C.8.7 Address Issues Related to Poor Connectivity

Please describe your approach for dealing with users in remote locations with poor, limited, or unstable internet connectivity (e.g., satellite, poor wireless coverage). Specific requirements for Poor Connectivity may be identified in the individual Task Orders.

C.8.8 Support or Provide Hardware Clustering

The Contractor shall provide capability to configure physical resources in a hardware cluster with a user configurable number of physical servers in the cluster. Specific requirements for Hardware Clustering may be identified in the individual Task Orders.

C.8.9 Provide Load Balancing

The Contractor shall provide the ability to distribute demand over multiple system instances. Specific requirements for Load Balancing may be identified in the individual Task Orders.

C.8.10 Support or Provide Interfaces to Non-Department Systems

The Contractor shall provide the ability to connect a Contractor hosted system or data store (“System A”) to another system (“System B”) that is hosted outside the DOI boundaries – example hosting locations include, but are not limited to:

- a. Another government agency
- b. A university
- c. A private sector enterprise

The connection, up to and including the Contractor boundary, shall be configured to support data exchange with System B. This shall include, but is not limited to, any necessary DMZ, firewall, gateway configurations and maintenance.

The connection shall support authentication schemes required by either System A or System B. Included, but not limited to:

- a. Active Directory
- b. OpenID
- c. Any other authentication schemes referred to in C.5.3 Establish and Maintain Security and Privacy

The connection shall adhere to all DOI security requirements including, but not limited to:

- a. Encryption of all sensitive data in transit (motion) and at-rest (storage) using only NIST Validated FIPS 140-2 compliant and validated cryptographic modules and algorithms.

Specific requirements for Interfaces to Non-Departmental Systems may be identified in the individual Task Orders.

C.8.11 Support or Provide Static IP Addressing

The Contractor shall provide a static IP for a specified compute host instance. Specific requirements for Static IP Addressing may be identified in the individual Task Orders.

C.8.12 Provision Dedicated Resources

The Contractor shall provide the option to provision dedicated as well as shared units of the resources. Dedicated resources are defined as physical resources for which the provisioning system is the sole tenant. Specific requirements for Provisioning Dedicated Resources may be identified in the individual Task Orders.

C.9 ASSOCIATED SUPPORT SERVICES

Associated support services are those services which may be required to enable identification, analysis, prioritization, preparation and migration of IT systems from the current operating environment to the target operating environment, or may be required to ensure sustained operations and maintenance of systems in the target operating environment. Categories for Associated Support Services are more completely described in Table 18 Associated Support Services.

Table 18 Associated Support Services

- C.9.1 Planning Services--- includes cloud readiness evaluation for QASP & Pilot Transition Plan
- C.9.2 Engineering Services
- C.9.3 Migration Services---includes Management of Cloud Transition, Pilot Transition
- C.9.4 Application Management Services
- C.9.5 Interface Design and Integration Services
- C.9.6 Testing- section 508 compliance
- C.9.7 Training Services
- C.9.8 Security Services

Specific requirements for Associated Support Services may be identified in the individual Task Orders.