DRAFT

Acquisition Professional's C.A.S.T.L.E. Guide

Cloud Adoption Survival, Tips, Lessons Learned, and Experiences Guide

DRAFT

This document, the Cloud Acquisition Professional’s Cloud Adoption Survival Tips, Lessons, and Experiences (CASTLE) Guide, is authored in partnership with Cloud Center of Excellence (CCoE).

Purpose: The CASTLE Guide supports program managers (PMs), contracting officers (COs) and other stakeholders in federal acquisition planning for cloud computing services. The CASTLE Guide assumes that the decision to pursue a cloud computing based IT solution has been made and that the associated analysis, tradeoff comparisons, business cases, and other appropriate IT business process analysis have all justified a cloud approach.

Description: The CASTLE Guide approach defines a representative set of conditions and allows agencies to match their condition to the different sets provided. Those conditions are matched to a corresponding and coordinated set of acquisition information that constitute scenarios within the guide. The agency may then leverage the information provided within the guide as acquisition-based guidance, but will need to tailor and supplement the information. The guide takes a narrow scope which includes targeted acquisition based topics proven to be problematic in the procurement of cloud computing services.

The guide’s scope is not all-inclusive nor comprehensive, but focused. The topics covered are the areas within an acquisition context that have proven, through experience and research, to have erected barriers to cloud acquisition for agencies. The expectation is the information in the Playbook will allow agencies to mitigate and smooth the acquisition process, thus increasing adoption of cloud services within the Federal Government.

Table of Contents

Table of Exhibits

1. *Introduction*

The Federal Government has developed strategies to increase the security and value of its information technology (IT) investments. Cloud computing is one of the primary approaches that is cross-cutting and broadly applicable. The advantages cloud can deliver to the Federal Government have generated both interest and intent to move onto cloud. However, the term “cloud” can create uncertainty or confusion, particularly to those lacking significant experience and education in this area. Some areas of uncertainty include how to apply contract types to meet cloud goals, how the market is structured, unfamiliarity with cloud models, and disconnects between cloud requirements and existing agency policies. These factors create the perception of barriers and slow the adoption of cloud within the Federal Government more than is desirable or sustainable.

Advantages of Cloud Computing

- Less expensive than maintaining physical infrastructure
- More agile than on-premise systems
- Provides greater scalability for surge and future demands
- Greater security

CCoE research and experience indicates that most inhibitors to federal cloud adoption are not technical in nature, but are the result of cultural constraints. Highly effective methods to address knowledge, understanding, and application of cloud computing increase the velocity of adoption for cloud computing in the Federal Government. A Guide that identifies, explains, and offers flexible paths to cloud acquisition and adoption effectively reduces or removes these barriers to increased cloud deployment. The Guide is scenario-based and explains a certain connected set of issues that provide a firm foundation and clear understanding of how to apply cloud technology in the Federal Government. Agency stakeholders can match key attributes of their agency’s expected situation to attributes of the provided scenarios that best illuminates potential guidelines, considerations, and a path forward for their agency. The guidelines, considerations and path-forward information are compact and succinct to facilitate more effective agency action. Should agency stakeholders have less familiarity with cloud and require more detailed information, the Guide provides layered details of information and background in Discussion, Expanded Topics, and Advanced Cloud sections. Cloud is a contemporary technology that applies Information Technology capabilities with highly variable usage that stretch perceived regulatory limits in areas like funding or contract types. To this end, the Guide provides thoughtful insights on the application of regulations to the cloud environment pertaining mainly to paying for cloud.

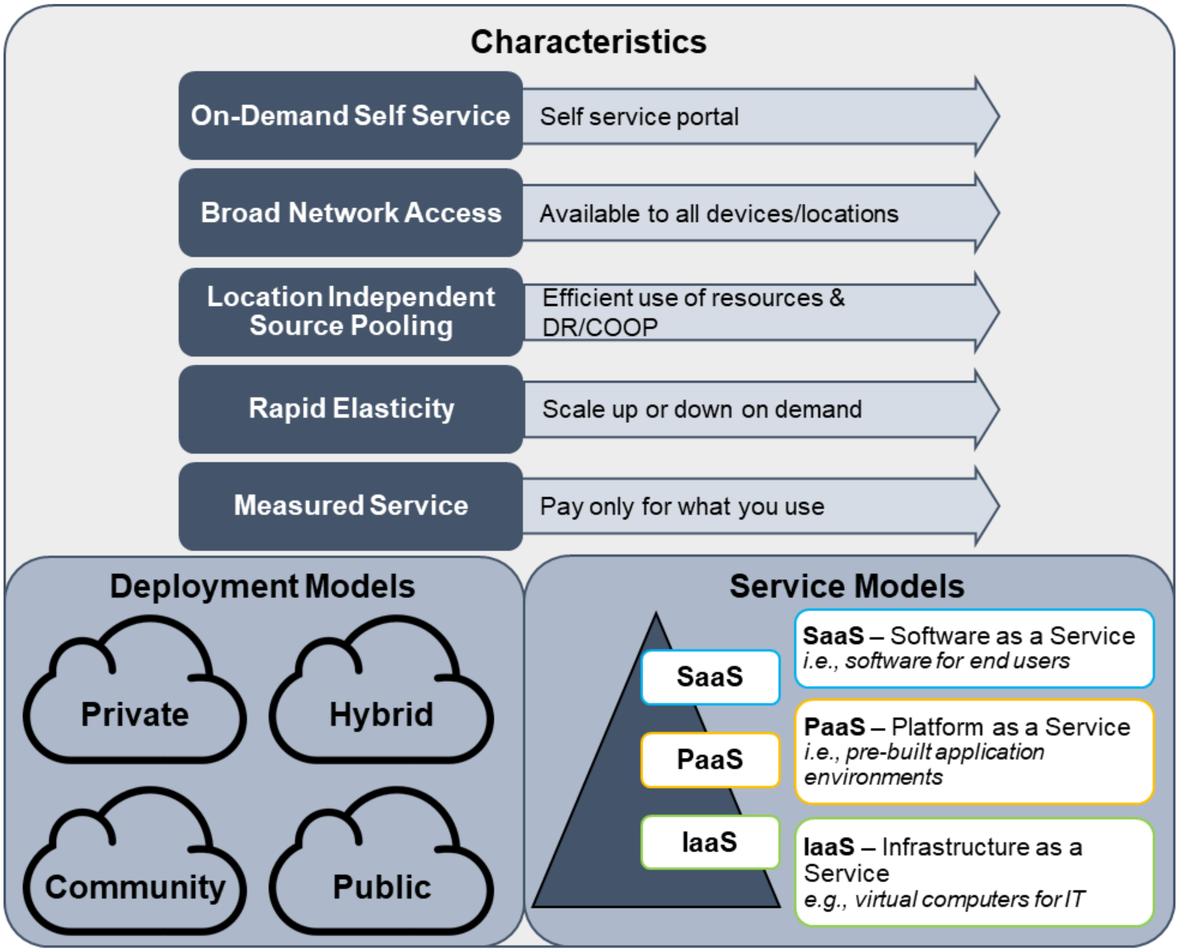
With the Guide, executive sponsors, program managers (PMs), contracting officers (COs) and their staffs can clearly understand and be confident about their cloud deployments. The Guide purposefully covers a prescribed set of topics that address the concerns of key agency staff involved with cloud deployment including those directly involved in the planning, application, and procurement of cloud computing services.

1.1 Cloud Computing Defined

“Cloud” has been used for many different architectures, services, functions, and applications. We define the term “cloud computing” per National Institute of Standards and Technology (*NIST) SP 800-145, The NIST Definition of Cloud Computing:*[1]

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

EXHIBIT 1 - NIST DEFINITION OF CLOUD COMPUTING


Characteristics
On-Demand Self Service
Self service portal
Broad Network Access
Available to all devices/locations
Location Independent Source Pooling
Efficient use of resources & DR/COOP
Rapid Elasticity
Scale up or down on demand
Measured Service
Pay only for what you use
Deployment Models
Private
Hybrid
Community
Public
Service Models
SaaS
PaaS
IaaS
SaaS – Software as a Service
i.e., software for end users
PaaS – Platform as a Service
i.e., pre-built application environments
IaaS – Infrastructure as a Service
e.g., virtual computers for IT

Source: NIST, DRAFT Special Publication 800-145

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

While this Guide endorses the computing services that are fully compliant with the NIST cloud characteristics, the concepts within this Guide apply equally well to any XaaS “Everything-as-a-service” (See Glossary) that have consumption-based pricing, fully eliminate related capital expenditures, and present packaged services consistent with commercial best practices.

1.2 Challenges of Cloud Computing

Commercial-ready cloud services are relatively new to the mass market. Cloud computing has no dedicated international standard and few conventional standards across vendors and the industry. Some of the existing challenges are the differences among cloud models, how the industry is organized, pricing practices, data rights, service definitions, and security. Many of these topics are covered in more detail in the Expanded Cloud Topics section of this Guide. However, consumption-based payment is one topic best covered early in the discussion.

Consumption-based payment is a fundamental component of cloud computing. Typically, an organization uses the service throughout the month and pays a metered rate that directly reflects what the organization used that month. The organization pays according to what it consumed.

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

EXHIBIT 2 - COMPARISON OF FUNDING MODELS

Funding Cloud in Private Enterprise	Funding Cloud in Public Enterprise
Pays for cloud with “consumption-based” model using metered billing	Constrained by budgeting and spending regulations and cannot utilize true “metered” services
Flexible budgeting cycles and methods	Restricted budgeting based on FY
Utilize business-to-business contracts that allow for front-loading and cost overruns	Cannot incur obligations in excess of contract funding
Ability to move funds easier to cover costs of demand surges or quick scaling	Must obligate a set amount of funds that may not cover full demand or may overestimate and leave money on the table

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

2. Core Cloud Guide

2.1 Visual Scenario Reference

Federal agencies face a common set of situations when deciding to acquire cloud solutions. This is the basis for the scenario-based approach that this Guide takes. The most common instructive situations are reflected in Exhibit 3, Visual Scenario Reference below. Usually, the situation and needs of an agency can be organized into four categories of services:

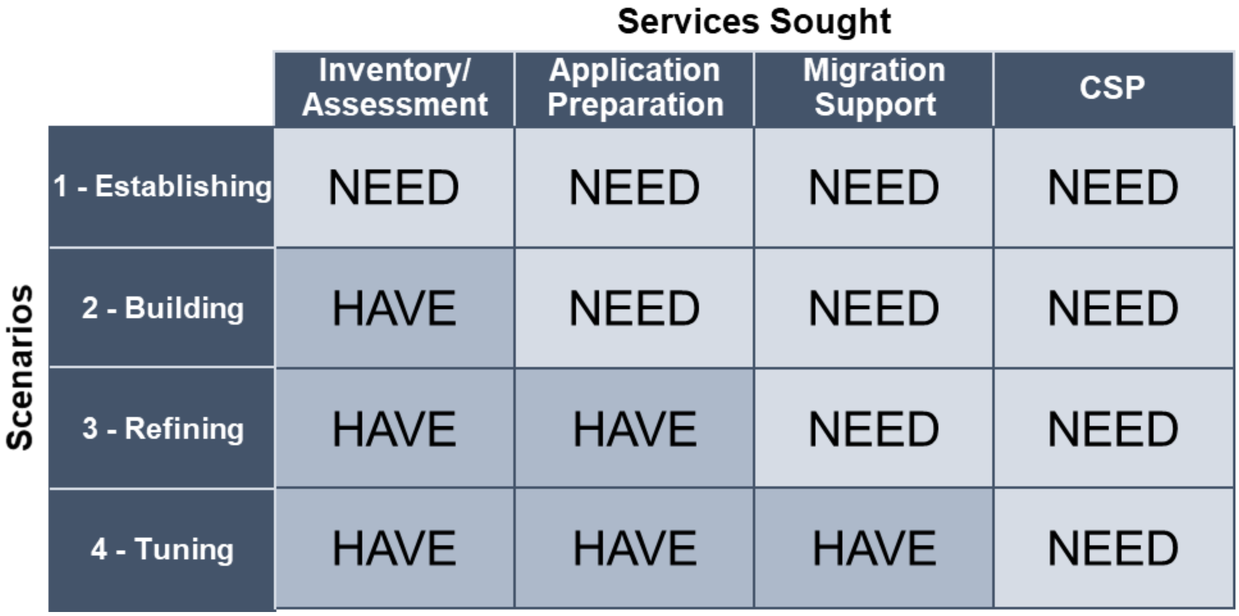
- **Inventory Assessment.** A formal, documented, and current record of applications and IT assets with corresponding descriptive attributes.
- **Application Preparation.** Applications that will be moved into the cloud are refactored, modernized, and certified to run in a cloud.
- **Migration Support.** A determination regarding how the migration will be performed - whether internal agency resources will perform the migration to the cloud or this work will be sourced.
- **CSP.** The agency will obtain the core cloud computing services (e.g., hosting) from the cloud service provider (CSP).

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

2.1.1 To Use the Guide

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

EXHIBIT 3 - VISUAL SCENARIO REFERENCE



Services Sought

Scenarios	Inventory/ Assessment	Application Preparation	Migration Support	CSP
1 - Establishing	NEED	NEED	NEED	NEED
2 - Building	HAVE	NEED	NEED	NEED
3 - Refining	HAVE	HAVE	NEED	NEED
4 - Tuning	HAVE	HAVE	HAVE	NEED

2.2 Scenario Structure

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

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

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

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

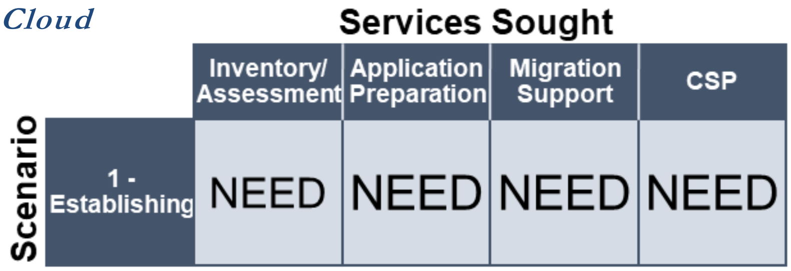
Key Questions. The list of key questions prompts topics and guidelines that are likely to increase success of a cloud acquisition. The information here expands on key information and topics in the Checklist and is broader in scope to provide a line of thinking that eases acquisition and increases likelihood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

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

2.3 Scenarios

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

2.3.1 Scenario 1: Establishing Cloud



Services Sought

Scenario	Inventory/ Assessment	Application Preparation	Migration Support	CSP
1 - Establishing	NEED	NEED	NEED	NEED

2.3.1.1 Initial Conditions:

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

2.3.1.2 Additional Assumptions

- Agency staff and support contractors have application support expertise, but limited expertise or resources for executing application upgrade and migration tasks.
- Single acquisition and any existing support contracts will be only minimally leveraged.

2.3.1.3 Checklist

❑ Inventory and definition of both existing infrastructure services and infrastructure services to be deployed as part of the contract.

❑ Current enterprise and solution architecture documentation.

❑ Current application definition list.

❑ Application reconciliation plan.

❑ Network architecture and connectivity – Trusted Internet Connection (TIC) compliance is met and required common services for integrations are available within required service levels.

❑ Organizational knowledge development plan.

❑ Documented support plan during migration.

❑ Thorough market research for system integrators (SI).

2.3.1.4 Key Questions

- Will your current service level definitions accommodate this delivery plan?
- Is your security breach and notification plan thorough, compliant and resilient?

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

2.3.1.5 Discussion

2.3.1.5.1 Inventory and Assessment

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

There are three main elements within an inventory and assessment phase to provide a foundation and roadmap for modernizing the IT enterprise. The first is the inventory, gathered from both automated scans and stakeholders. This inventory documents all IT assets and provides both a physical and a logical organization to those assets such as by application system, environment (dev, production, etc.), circuit, physical location, and organizational control. The next element is the application rationalization which documents business functions and system integrations. The outputs are specific modernization plans and recommendations including eliminating duplicative systems by merging application functions, terminating legacy applications with minimal business value, and complete application re-engineering when warranted. The third element is the actual migration planning which is often constrained by budgetary considerations and necessarily considers risk assessments for prioritization. GSA developed at the request of OMB, and in collaboration with industry partners, a set of statement of objectives (SOO) templates for agency use in acquiring cloud migration support services such as assessment, planning, execution and decommissioning.[2]

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

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

2.3.1.5.2 Application Preparation

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

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

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

2.3.1.5.3 Migration Support

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

Network architecture and agency circuit capacity for the network traffic between agency premises and the CSP is a key planning element. Patterns vary widely for network traffic and utilization by applications based on the variety of types, number, and logical location (public, internal agency, trusted systems, etc.) of users and systems connecting as well as the amount of data transferred. The inventory and assessment phase considers these issues and can even indicate a scope change to the targeted migrated systems based on this information. Prior market research should inform whether a dedicated circuit to the CSP is warranted or if the overall network capacity should be within both LAN/WAN environments as part of the overall project. Anticipate coordinating appropriate changes to the existing agency telecom and circuit contract as the approach is determined. At a minimum, plan for the acquisition to specify development of networking architectures to ensure sufficient bandwidth and a TIC-compliant solution.[3] Note there can be challenges with some cloud-exclusive type architectures in meeting monitoring requirements contained in TIC, but it does remain a Federal requirement.

To the extent possible within this project and acquisition, executing a phased migration with the key support infrastructure moving first will lower risk more than performing a complete cutover of all targeted applications at once. Subsequently, migration of the four targeted applications individually may limit the scope of potential related mission delivery problems. Since moving a significant portion of IT services is contemplated in this project, a phased approach to effectively test networking, latency, and overall service performance is useful in potentially limiting the scope of affected systems with each change. Consider moving key support infrastructure first or early in the process to shed light on undocumented dependencies within the systems and applications that are

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

not in scope for migration in this phase. When it is architecturally feasible to do so, move individual components within an application in stages to mitigate cutover risk in the cases. Effective testing of production systems in new environments can be challenging and, given the mission critical nature of the targeted applications, these strategies may prove effective.

2.3.1.5.4 CSP

CSP specific requirements won't likely be numerous in a scenario where there is little agency cloud footprint and is the first significant foray for the agency into cloud. DR and COOP requirements are best treated at the application level versus viewing the CSP as a traditional datacenter and layering on outmoded legacy backup requirements. The goal is a transition to the cloud and an associated operational transformation to an efficient service oriented posture. Include a geographic diversity requirement; it is easily met by most CSP. Granted, not all (and perhaps even few) typical Federal agency applications will ever be re-engineered into fully next generation cloud-designed applications that are stateless works of resiliency but it still makes sense to position the organization to leverage this potential where appropriate. Focus CSP-specific specifications on items such as average resource deployment times, resource configuration requirements (e.g. VM's with 16 cores), resource performance (e.g. network and block storage IOPS), CSP Support levels (Gold, Bronze, Silver and Platinum), and functional characteristics such as fully API-enabled access to all capabilities.

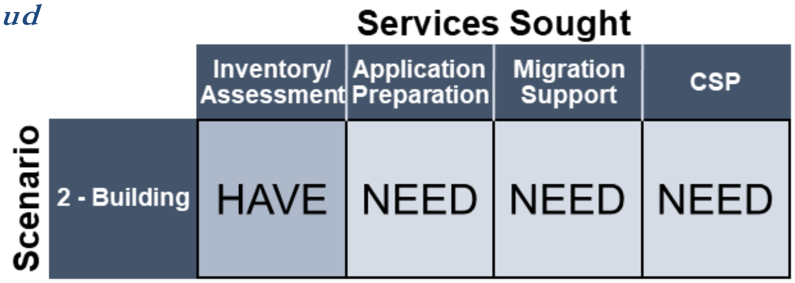
This scenario contemplates migration of four mission critical applications. Assign application availability SLA's to the contractor layering managed services above the CSP and not directly with the CSP hosting the resources. The implementation path the contractor chooses to achieve those service level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

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

2.3.1.5.5 Contract Vehicle Options

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

2.3.2 Scenario 2: Building Cloud



		Services Sought			
		Inventory/ Assessment	Application Preparation	Migration Support	CSP
Scenario	2 - Building	HAVE	NEED	NEED	NEED

2.3.2.1 Initial Conditions:

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

2.3.2.2 Additional Assumptions

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

2.3.2.3 Checklist

❑ Current enterprise and solution architecture documentation.

❑ Application reconciliation contract or internal work plan.

❑ Organizational knowledge development plan.

❑ Post-migration application support strategy.

❑ Network architecture and connectivity – TIC compliance is met and required common services for integrations are available within required service levels.

❑ Cost goals that reflect what is more expensive and what is less expensive when deploying cloud services.

2.3.2.4 Key Questions

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

2.3.2.5 Discussion

2.3.2.5.1 Application Preparation

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

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

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

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

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

2.3.2.5.2 Migration Support

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

2.3.2.5.3 CSP

The overall scope of the line of business application being migrated may consist of many subsystems creating a large footprint of VM’s, storage, and bandwidth consumed by the aggregated whole. This initial resource footprint will be further multiplied when factoring in the various environment instances required for a full development lifecycle such as for development, integration, quality assurance (QA), and production environments. Pricing the CSP is a challenge for the contractor. Compounding the contractor’s problem in pricing such services will be the phased approach of the project and potential significant unknowns in the application modernization and preparation phase that will impact resource consumption while seeking to maintain performance characteristics.

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

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

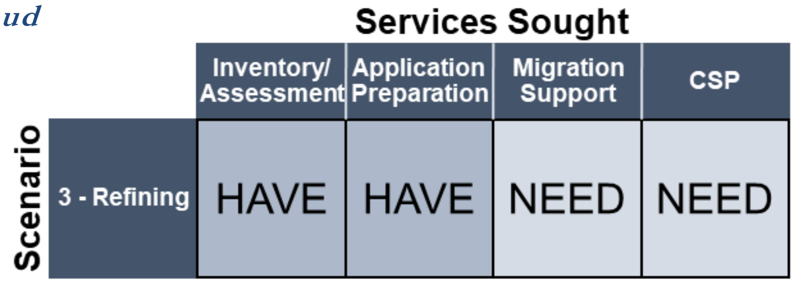
2.3.2.5.4 Contract Vehicle Options

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

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

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

2.3.3 Scenario 3: Refining Cloud



Services Sought

		Inventory/ Assessment	Application Preparation	Migration Support	CSP
Scenario	3 - Refining	HAVE	HAVE	NEED	NEED

2.3.3.1 Initial Conditions:

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

2.3.3.2 Additional Assumptions

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

2.3.3.3 Checklist

❑ Data rights and movement conditions are documented as a requirement.

❑ Documented support plan during migration.

❑ Post-migration application support strategy.

❑ Post migration support and communications plan for mission area application users.

❑ Network architecture and connectivity – TIC compliance is met and required common services for integrations are available within required service levels.

❑ Cost planning strategies.

2.3.3.4 Key Questions

- Is your security breach and notification plan thorough, compliant, and resilient?
- What are the changes you plan to make to disaster recovery and COOP plans?
- Will your service level definitions accommodate this delivery plan? How will you maintain surveillance and balance competing requirements?
- Are targeted applications cloud-ready?
- Do you have a requirements definition that clearly defines duties of the provider relative to duties of the government?
- Do you have a full understanding of affected software licensing that will move to the cloud?
- Are your administration rights, delegation, and credential issuing plans sound?
- Do you have the governance in place to manage provisioning (ordering) and de-provisioning of cloud services?

- Do you have a requirements definition that clearly defines duties of the provider relative to duties of the government?
- Do you have a comprehensive set of service level agreement requirements? Does it include acceptable application performance metrics?

2.3.3.5 Discussion

2.3.3.5.1 Migration Support

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

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

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

Consideration of a cloud management platform implementation, capable of supporting the multiple clouds deployed across the enterprise, is appropriate if one not is already in place. However, implementation of a successful cloud management platform may be better served as a separate project to enhance opportunities for solution flexibility rather than tacking it onto this acquisition.

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

2.3.3.5.2 CSP

This scenario represents a novel case where a particular CSP[4] is used for hosting, and a specific provider is purposely not leveraged to specifically provide for vendor diversity to enhance resiliency. The agency's national presence may increase the likelihood that some application or application interaction characteristics exist that necessitate a CSP with particular attributes such as multiple regions for potentially more localized resource deployment.

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

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

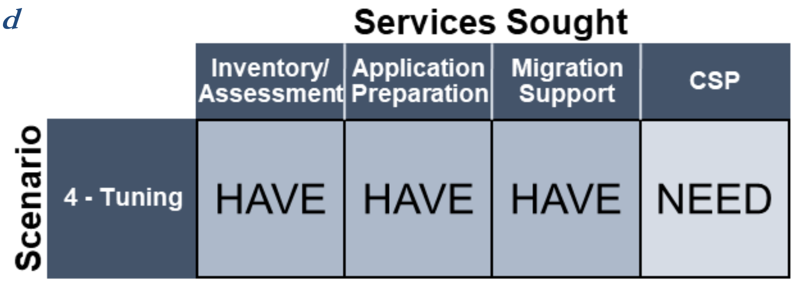
2.3.3.5.3 Contract Vehicle Options

There are many contracting vehicle options to meet the basic requirements of providing significant hosting capacity combined with considerable IT support labor to implement the transition. The biggest project specific factor that influences the available choices will be the number of systems moving and their interdependencies. These factors increase the overall amount of IT services support involved in the overall acquisition.

[4] CSP justification is discussed within other Scenarios.

Additionally, as this complexity increases, actual system transition execution phases may be introduced thereby lengthening overall implementation timelines and necessitating more sophisticated contract structures. These higher complexity enterprise level projects will favor the general-purpose IT solutions-based contracts (e.g. Alliant, CIO-SP3) over the delivery-order based GWACs (e.g., CIO-CS, SEWP). Cloud-focused contracts including transition support services such as DOI's FCHS or an available agency-specific option can be considered in addition to the utility belt of IT contracting, Schedule 70.

2.3.4 Scenario 4: Tuning Cloud



Services Sought

Scenario		Inventory/ Assessment	Application Preparation	Migration Support	CSP
	4 - Tuning	HAVE	HAVE	HAVE	NEED

2.3.4.1 Initial Conditions:

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

2.3.4.2 Additional Assumptions

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

2.3.4.3 Checklist

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

2.3.4.4 Key Questions

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

2.3.4.5 Discussion

2.3.4.5.1 CSP

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

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

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

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

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

2.3.4.5.2 Contract Vehicle Options

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

Contract vehicle access to CSPs differs based on the service model, especially for SaaS. Comprehensive IaaS providers that deliver a range of typical hosting services including various sized VM's, storage options, and flexible programmatic networking capabilities, are typically well represented on vehicles. SaaS providers may not be generally available on multiple government-wide contracts due to licensing exclusivity with their channel partners.

3. Expanded Cloud Topics

3.1 Cloud Services vs. Managed Data Center Services

The cloud market is nascent enough that there are general conventions, but few standards within the industry. As a result, many apply traditional understanding and historical frameworks to cloud services. It is common for those unfamiliar with the cloud industry to view cloud through the lens of managed services. This is much more familiar to them; they hear familiar terms and readily apply the managed services framework to increase their ease of deployment and speed of progress. While understandable, this may be a significant mistake.

A simple example of this situation is the service type and levels an agency receives when they purchase infrastructure managed services as part of a data center outsourcing arrangement. An agency expects to receive all services including physical structure, air conditioning, facility power distribution, network core and support, and server platforms. Maintenance of these components is reasonably expected as well. When purchasing cloud services, the maintenance of some components such as applications and monitoring services standardized to existing agency models and systems are not included in the standard CSP provided services.

Most cloud infrastructures are virtualized frames that run an “operating system” for the frame (hypervisor for example), typically referred to as the host. The cloud provider operates, maintains, and guarantees the host or frame management operating system as it is on CSP’s side of the service boundary. On the agency side of the boundary is the operating system (OS) known as the “guest” that runs the computing instances for the agency. The guest runs the agency application as part of the virtual OS and interfaces with the application. This is a modern form of the traditional OS most of us are familiar with from the “racked iron” era. By default, in the IaaS environment this guest OS is not necessarily patched, updated and maintained as a standard managed cloud offering as an agency might expect if viewing this through a managed service lens.

Standardized commercial CSP offerings efficiently support high volume consumption and perceived near-infinite scaling capabilities in a multi-tenant environment. Standardization typically means the agency consumer needs to have additional services layered on top of the direct CSP service to match their individual requirements. These additional services can be provided either by agency staff or by contracting for professional services. A common example exists in Infrastructure as a Service (IaaS) offerings such as a virtual machine service. Although IaaS CSP’s will provide the agency consumer with a fully tested and patched OS image to launch the virtual server, once that virtual machine is launched and running, the CSP is not responsible for installing application software, applying future OS patches, monitoring that the server is performing the task intended (e.g., software application errors), or otherwise responsible for management of what happens within that guest server instance. These extra services, along with other requirements such as disaster recovery, continuity of operations, and application management, constitute typical managed data center services.

Planning for these services in the cloud space is a key procurement and risk management consideration. Does your agency have in-house expertise to provide these services or are they currently contracted to a system integrator? Although they can easily be obtained and contracted with the IaaS hosting services by system integrators or other contractors, consider tradeoffs in contracting convenience versus flexibility and managing vendor lock-in risk by separating the contracting efforts.

3.2 Transition Professional Services

Transition professional services include IT professional services used to support the migration or transition of workloads from its current hosting environment to a destination environment. This includes support services such as inventory, assessment and rationalization, migration assistance, cloud architecting, environment configuration, and similar related services. Usually, CSP rates for compute, storage, or related provisioned resources include billing administration, help desk specific to services within the CSP's boundary, incident response, etc.

3.3 Paying for Cloud

3.3.1 Consumption-based Billing

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

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

3.3.2 How the Government Pays for Cloud

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

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

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

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

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

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

3.3.3 Approach 1: Optional CLIN Not to Exceed:

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

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

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

3.3.4 Approach 2: Drawdown Accounts:

Drawdown Model A: Government monitors

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

Drawdown Model B: Vendor monitors

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

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

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

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

3.3.5 Approach 3: Subscription Based

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

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

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

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

3.3.6 Conclusion

The Federal government’s existing methods of buying cloud services (i.e., optional CLINs, drawdown accounts, and subscription models) do not effectively address the problem of demand elasticity and portability. They are ultimately minor variants in contracting structure, business financial process emphasis, or product re-characterizations that only help incrementally by shifting trade-offs without providing complete solutions. None of these methods provide for a complete realization of benefits of cloud computing by providing effective means for the government to both consume and pay only for the resources it needs and uses. A potential solution to this might explicitly allow for cloud computing resource units to be treated, including associated oversight risk, like labor hour rates (fixed unit price) in T&M contracts.

3.4 Cloud Security Considerations

Providing for the security of IT systems is a well-established process within FISMA. Cloud computing necessitates fresh approaches for implementing IT system security versus traditional on-premise deployment methods. The following cloud security considerations focus attention on those topics most likely to be affected by the shift to a cloud computing model.

3.4.1 Risk Assessment

Any agency or organization contemplating a move to cloud computing needs to perform a security risk assessment. Questions regarding data type and classification, data hosting and storage, and business continuity need to be addressed early in the procurement process.

When using a GWAC or other IDIQ purchasing vehicle, individual or specific security requirements need to be addressed at the task order (TO) level.

3.4.2 Data Types

Security categorization of the data needs to be addressed when considering cloud migration. Security categorization and mission criticality will determine what type, size, and flavor of cloud computing the customer agency will want to consider.

3.4.3 Geolocation

Do you know where your cloud files are? Or where they will be? More importantly, what are the policies of your agency on the matter? Due to the rapid implementation of cloud computing, many agencies are behind in development of policies pertaining to cloud storage and hosting. Many cloud service providers have data centers that span the globe and some CSPs utilize distributed storage systems. When choosing your cloud service provider consider whether your data must be stored under the jurisdiction of the United States..

3.4.4 Personnel

Another critical security area to consider when moving to the cloud is the need for personnel. Do you have the expertise in house to manage your cloud implementation? Does your agency have citizenship requirements for employees? Are you aware that some CSPs have help desk personnel in locations outside of the continental US? Will your CSP have access to your data or will you encrypt everything before storing it? (In the case of Storage as a Service)

3.4.5 Compliance Issues

A cloud computing environment, whether self-provided or provided by a third-party, must adhere to all applicable government security guidelines and mandates just as with a traditional on-premises environment. As an extension of the on-premises environment, the cloud computing environment must pass through the Security Assessment and Authorization (A&A) process with the final product being an Authorization to Operate (ATO) that the agency itself must sign off on deeming the risk to operate the system as acceptable.

.

Third-party CSPs may be considered for a Joint Authorization Board (JAB) Provisional Authorization to Operate (P-ATO). These are issued by the Federal Risk and Authorization Management Program, or FedRAMP which provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

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

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

These same scenarios apply to ATOs issued by other agencies which may also be leveraged by the purchasing agency.

3.4.6 Other Technical Considerations

While there are many common risks to evaluate, technical considerations still remain. Be sure to ask your potential CSP about the following:

- **Application and Service Portability** – Difficult for customer to migrate from cloud service provider to another or back to in-house.
- **Isolation Failure** – Failure of service providers' mechanisms that separate storage, memory, and routing.
- **Management Interface Compromise** – Management interfaces of public clouds are often Internet accessible and pose additional risk when combined with remote access and browser vulnerabilities.
- **Data Protection** – The customer has no real insight into the CSPs data handling practices.
- **Insecure or Incomplete Data Deletion** – In the case of multiple tenancies and the reuse of hardware resources there is a risk of untimely or inadequate data destruction.
- **Malicious Insider** – Cloud architectures require roles that are extremely high risk, and the potential damage caused by a malicious insider could be far greater.

OMB mandates that all agencies use only CSPs that are compliant with FedRAMP security standards for their cloud computing needs. It is important for agencies to write this into their requirements documents and solicitations as directed and provided by FedRAMP.[5]

3.5 Legal and Contractual Concerns

There are a host of important legal and contractual clauses to consider when selecting and acquiring a cloud service. To fully utilize Federal best practices and lessons learned and to simplify the acquisition process, refer to the excellent report by the CIO Council and the Chief Acquisition Officers Council, "Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service." [6] This document contains a substantial amount of useful information and should be an agency's first resource on legal and contractual topics such as:

- CSP and End User Agreements
- Service Level Agreements
- Privacy
- E-Discovery
- FOIA Access
- Federal Recordkeeping

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

3.6 Data in Clouds

3.6.1 Data Residency

The physical location of where the data resides is an important factor to consider. Though the data resides in the "cloud," an agency may still have requirements (legal, regulatory, or architectural) or preferences about where the data is located that should be specified to the CSP during the negotiation of the purchase. For example, a critical requirement for some agencies is that the data reside in the contiguous U.S. (CONUS) and not be routed through or stored on infrastructure outside of the contiguous U.S. (OCONUS), as can happen when selecting a CSP with global infrastructure. Whatever the requirement may be, it should be clearly communicated with the CSP and written into the contract to ensure obligations are met.

3.6.2 Data Ownership / Rights

Another critical requirement is ensuring that the agency acquiring cloud services retains ownership to the data it stores and the rights to access, modify, or migrate that data if and when it chooses. Such an agreement ensures that the Government can select and migrate to another CSP if it is not satisfied with the services it receives. This point must

[5] https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/03/FedRAMP_Standard_Contractual_Clauses_062712_0.pdf

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

always be made clear with the CSP prior to the acquisition and specified in writing in the final contract.

Ownership rights are especially important to negotiate beforehand to address potential data breaches. It is a best practice to ensure that the CSP is held accountable for data breaches, even as they do not own the data. According to the CIO Council and the Chief Acquisition Officers Council, "Federal agencies should make explicit in cloud computing contracts that CSPs indemnify Federal agencies if a breach should occur and the CSP should be required to provide adequate capital and/or insurance to support their indemnity. In instances where expected standards are not met, then the CSP must be required to assume the liability if an incident occurs directly related to the lack of compliance."[7]

Greater detail on data ownership and rights pertaining to termination of service, breaches, and information and records management can be found in the CIO Council report.[8]

3.7 Choosing a Requirements Document Type and Solicitation Type

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

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

Many agencies use a SOO which states the agency goals in the most general sense, allowing vendors more creativity in proposing a solution. For instance, instead of naming the number and type of processors needed, the amount of memory and storage, etc., only the projected usage statistics of an application are named. Usage statistics such as the number of visits to a website per day, the average page size, the average number of pages viewed per visit, etc., are provided in a SOO.[9]

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

[8] Ibid.

[9] Additional detail on requirements documents is at https://www.gsa.gov/MASDESKTOP/section7_3.html.

Exhibit 4 - Requirements Document Type Benefits

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

In general, for cloud computing, a SOO issued within an RFQ would suffice. That way, the vendor solutions contained in responses can be innovative yet contain specific pricing. If the agency wishes simply to establish an agency "gift card" type of drawdown account with funding attached to a CSP then this may be an optimum solution. CSPs may respond with their full price list of available services, which the agency can pick and choose from at the task order level.

The final selection of the SOO, SOW, or PWS is authorized by the ordering CO based on the characteristics of the acquisition. It is important for the IT shop or program office to engage with their CO early in the process because decisions like these need to be made throughout this process.

3.8 Cloud Service Models and Contract Types

There are three service models as defined by NIST: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These service models are vastly different in use characteristics from the consumer standpoint. As such, these models may require different approaches to be better managed and paid for under different conditions or contract types. The two most common contracts types for cloud service models in the Federal Government are T&M and FFP.

Consider the service models required; and then determine the subcategories of those service models. Consider IaaS and PaaS together, and SaaS on its own. The two subcategories to consider under IaaS-PaaS are whether or not IT professional services are needed in support of the service model. For SaaS, consider the subcategories as seats and usage, but IT professional services are still an important consideration depending on the service. This sets up a framework for an appropriate discussion of cloud service models and contract types.

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

SaaS offerings vary from IaaS and PaaS in that vendors typically charge for active users or seat licenses that are permitted to access the service. SaaS seats may be scaled up or down each month in keeping with the metered billing model for use in a T&M or FFP contract. To take advantage of the SaaS cost savings, a T&M contract type should be used to pay for usage. Most SaaS offerings include monitoring capabilities built into the service. Agencies can take advantage of the automation tools to help provision, control access, and provide cloud monitoring and reporting. It may be difficult to get agency CO buy-in as the FAR imposes limitations on T&M contracting. If an agency selects a FFP contract type for a SaaS procurement, allow for the flexibility at the CLIN or TO level so cost savings can be realized.

Exhibit 5 - Service Model Contract Type Considerations

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

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

3.9 Risks of Not Buckling Your Seatbelt

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

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

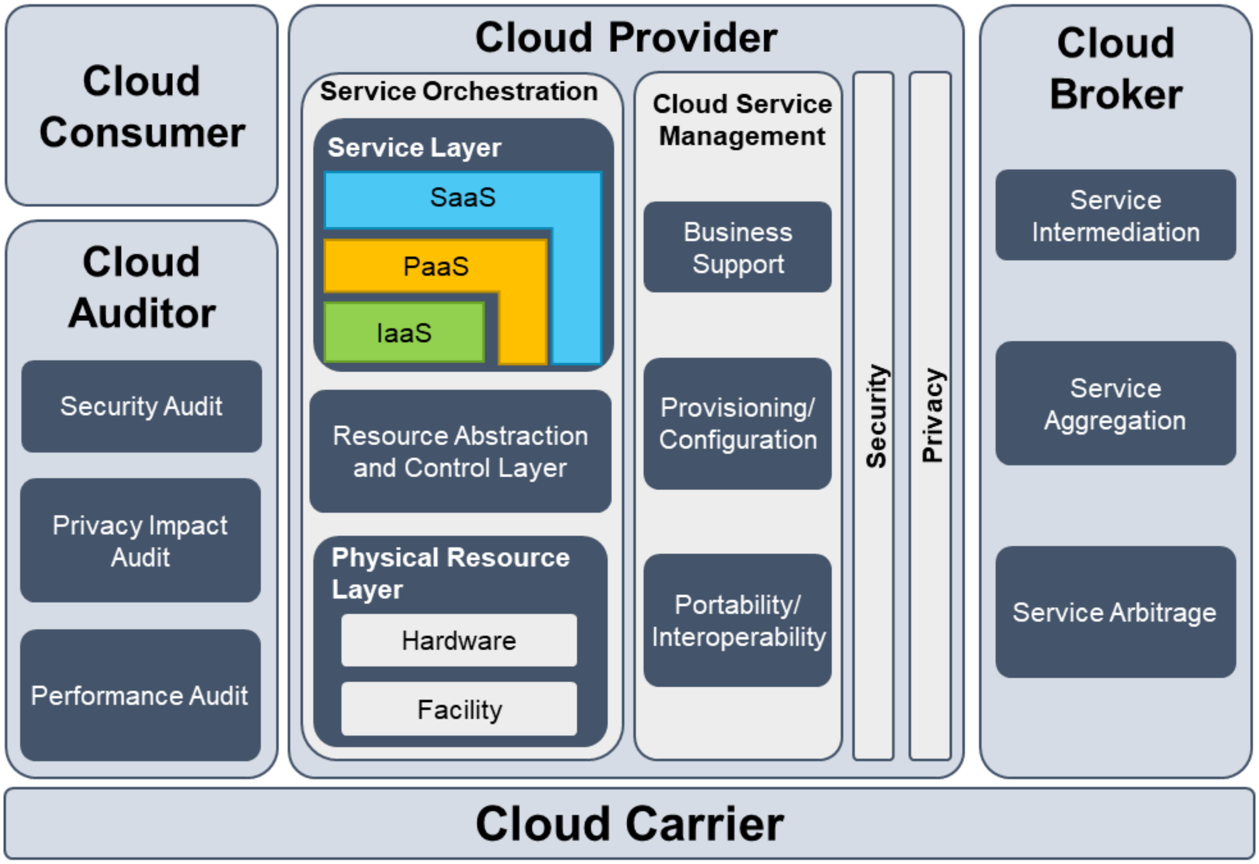
Additionally, these resources are quickly spun up are sometimes not spun back down, leading to wasted resources and unnecessary expense. Easy scalability without proper governance can lead to the government committing to a large sum of money. There can be instances where scaling up for resources are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

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

3.10 Cloud Responsibilities

Clarity in roles and responsibilities is a basic and very important factor for any well-run IT service and organization, but it may be more important in the cloud environment than in many legacy computing environments. The reasoning being cloud is relatively new, and responsibilities in a new paradigm need to be established. There is a need to lower risk exposures inherent in cloud’s low friction scalability environment. Finally, new roles are needed that emphasize and bring new skillsets to the forefront. Agencies should consider the following roles and responsibilities as fundamental to a well operated and well governed cloud environment.

EXHIBIT 6 - NIST CLOUD REFERENCE ARCHITECTURE



3.10.1 Cloud Broker

The Cloud Broker is an individual or organization that consults, mediates, and facilitates the selection of cloud computing solutions on behalf of an organization (in this federal example case, an agency e.g., USDA). A cloud broker is an entity that manages the use, performance, and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers.

3.10.2 Cloud Carrier

The Cloud Carrier is the intermediary that provides connectivity and transport of cloud services between Cloud Service Provider(s) and Cloud Consumers.

3.10.3 Cloud Auditor

The Cloud Auditor is the organization that can perform an independent examination of cloud service controls with the intent to express an opinion thereon. Audits are performed to verify conformance to standards through a review of objective evidence. A cloud auditor can evaluate the services provided by a cloud provider such as security controls, privacy impact, and performance.

3.10.4 Cloud Service Provider (CSP)

The Cloud Service Provider can be a person, an organization, or an entity responsible for making a service available to cloud consumers. Their services are categorized as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS) and are provided to other businesses or individuals.

3.10.5 Cloud Consumer

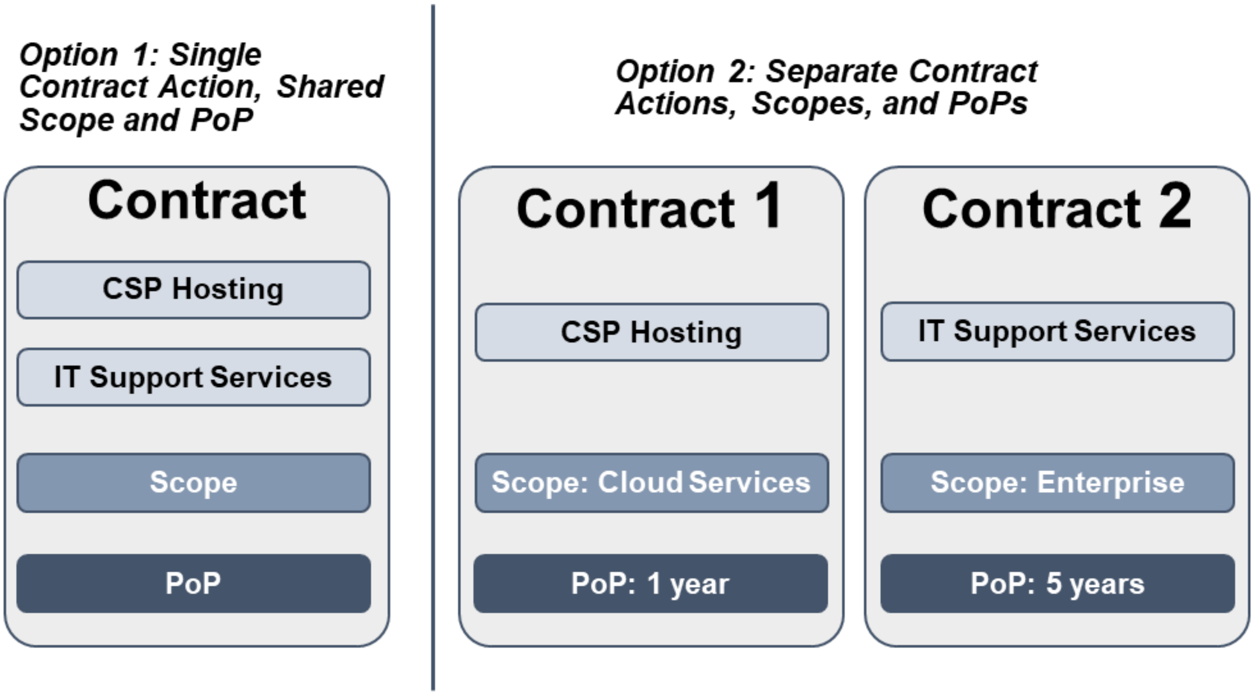
The Cloud Service Consumer is the ultimate stakeholder that the cloud computing service is created to support. A cloud consumer represents a person or an organization that maintains a business relationship with and uses the service from a cloud provider.

4. Advanced Cloud Topics

4.1 Strategic Contracting Considerations

While the scenarios in this Guide used an assumption of a single contract to procure and execute the entire scenario, there are many other contracting permutations that agencies might leverage in their cloud environment. The types of services that providers offer to organizations will continue to grow. The Guide recommends consideration of using multiple procurements to separate the cloud professional services from the hosting services. Doing so allows agencies to swap out CSPs without interrupting the work being done by the cloud professional services contractor or vice versa preventing vendor lock-in.

EXHIBIT 7 - CONTRACT OPTIONS REPRESENTATION



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

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

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

All cloud services must implement the FedRAMP cloud security baseline controls. These controls are represented in the necessary contract language available on the FedRAMP website. It is important to note that current Federal (but not DoD[10]) policy does not require the cloud service offering to already have a demonstrated FedRAMP authorization at the time of award. The standard contracting language requires that the vendor have the capability to comply with the FedRAMP standards at award. However, in the interest of speed to deployment of the cloud services, or for other reasons, an agency may require that the CSP already possess a FedRAMP authorization to be

[10] DoD-originated acquisitions require any Cloud Service Offering (CSO) to already possess a Provisional Authority (PA) at the appropriate Impact Level per DFARS Subpart 239.7602-1(b)(1)

eligible for contract award. For this requirement to withstand protest and meet fair opportunity requirements there must be a sufficient number of contractors capable of meeting the overall contract requirements. This constitutes an additional factor that may trigger limited source justifications.

4.2 Blanket Purchase Agreements

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

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

The DHS Enterprise Computing Services (ECS) BPA is a prime BPA example. ECS provides Cloud Hosting Services for the agencies under DHS, and allows for terms and conditions to be set at the BPA level as any solution offered on the BPA must be FedRAMP authorized. Agencies can leverage the BPA for recurring requirements under separate task orders that provide DHS an opportunity for leveraging further discounts at the TO level.

IDIQs can apply across a host of opportunities and should be considered as a viable procurement strategy. For example, the Army ACCENT[11] Multiple award IDIQ has many characteristics that fit a BPA procurement strategy such as recurring transition requirements. Army wanted a standard tool that preset all the base requirements for their estimated 10,000 applications that are to be migrated to the cloud. The contract requirements included IaaS, SaaS, and PaaS offerings and had offerors demonstrate a

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

DISA issued Provisional Authority for award. It further included in scope all the IT professional services needed to fully support and execute the transition and migration of these applications. Although ACCENT was not itself executed as a BPA, it is an excellent example of a use case for a cloud BPA that includes migration services in contrast to the DHS ECS BPA which is limited to CSP services.

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

5. Selected References

- Army, Army Cloud Computing Strategy, March 2015
- CIO Council, Creating Effective Cloud Computing Contracts for the Federal Government, February 2012
- CIO Council, Federal Shared Services Implementation Guide, April 16, 2013
- DISA, Best Practices Guide for Department of Defense Cloud Mission Owners, August 2015
- DoD, Department of Defense Cloud Computing Security Requirements Guide (SRG) v1r3, March 6, 2017
- DoD, Department of Defense Cloud Computing Strategy, July 5, 2012
- GAO, GAO-16-325, CLOUD COMPUTING: Agencies Need to Incorporate Key Practices to Ensure Effective Performance, April 7, 2016
- GSA/OMB, Cloud Migration Services SOO Templates, December 2012
- NIST, NISTIR 7956, Cryptographic Key Management Issues and Challenges in Cloud Services, September 2013
- NIST, SP 500-299, NIST Cloud Computing Security Reference Architecture (Draft)
- NIST, SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010
- NIST, SP 800-125, Guide to Security for Full Virtualization Technologies, January 2011
- NIST, SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing, December 2011
- NIST, SP 800-145, The NIST Definition of Cloud Computing, September 2011 (errata as of 161 April 27, 2012)
- NIST, SP 800-292, NIST Cloud Computing Reference Architecture, September 2011
- NIST, SP 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010 (Updated 6/5/2014)
- NIST, SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (includes updates as of 01-22-2015)
- NIST, SP 800-53A Revision 4, Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans, December 2014
- NIST, SP 800-60, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008
- OMB, 25 Point Implementation Plan to Reform Federal Information Technology Management, December 9, 2010
- OMB, Federal Cloud Computing Strategy, February 8, 2011
- OMB, Federal Information Technology Shared Services Strategy, May 2, 2012
- OMB, Guidance on Exhibit 53—Information Technology and E-Government, July 1, 2013

- OMB, Memorandum for Chief Information Officers, Security Authorization of Information Systems in Cloud Computing Environments, December 8, 2011
- OMB, Memorandum for Federal Chief Information Officers, Increasing Shared Approaches to Information Technology Services, May 2, 2012

6. Glossary of Terms[12]

Application Refactoring. The product of modifying an existing code base to significantly improve the performance and technical architecture of the code; and is not primarily motivated to change the code functionality. Typically, this is an aggregate set of refinements, enhancements, and modifications that are potentially not justified by resource input to perform alone, but are expected to have a major improvement when performed holistically. Changes, modifications, and enhancements can include elements such as database changes and code reorganization.

Cloud Enabled. A software application or workload that is both ready to be hosted in an IaaS (or PaaS) cloud environment and has some capability to leverage the cloud characteristic of rapid elasticity. The expectation is of only a minimal amount of configuration effort would be required to deploy (or re-deploy) the application in the cloud.

Cloud Service Provider. A service provider that owns, maintains and enhances their services, and houses those service elements in a location that they own. Service is usually delivered via the internet or other network connection. Customers usually pay on a routine cycle and at a rate usually based on their usage that period or at a recurring standard rate.

Drawdown Accounts. An organizational method for paying for a cloud service. The consuming organization pays the provider a set amount of money. The provider decrements the money put into the account relative to what the consuming agency is using.

IaaS. A service model describing an offering from a provider that allows a customer to purchase compute, storage and network services on demand. IaaS is priced by a consumption unit. The customer pays for the service used during the period based on a per consumption unit price.

PaaS. A service model describing an offering from a provider that allows a customer to make on demand purchases. The types of services included in this model are broad and loosely defined as those infrastructure and end user applications. PaaS is priced by a consumption unit. The customer pays for the service used during the period based on a per consumption unit price.

SaaS. A service model describing an offering from a provider that allows a customer to purchase the use of the software on demand. The software has a single code base and

[12] Expanded cloud definitions available in NIST SP 800-292 *NIST Cloud Computing Reference Architecture*.

is available to many different organizations and individuals that may or may not be affiliated. SaaS is priced by a consumption unit. The customer pays for the amount of service used during the period as a function of the price consumption unit or by a standard subscription fee.

Subscription Based. A payment arrangement between a provider and customers. Consumers and consuming agencies pay a fee to access the service the user provides. This payment type is not based on how much the consumer uses, but whether or not the user has on-demand access to use the service.

7. Appendix: Representative Example Contract Clauses

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

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

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

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

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL	Add'l info req'd
Asset Availability	(1) The Contractor must inform the Government of any interruption in the availability of the cloud service as required by the service level agreement.			X		X		
Asset Availability	(2) Whenever there is an interruption in service, the Contractor must inform the Government of the estimated time that the system or data will be unavailable. The estimated timeframe for recovery of the service must be related to the FIPS 199 system categorization for the availability of the system and if specified, agreed upon service level agreements (SLA) and system availability requirements. The Contractor must provide regular updates to the Government on the status of returning the service to an operating state according to the agreed upon SLAs and system availability requirements.			X		X		
Asset Availability	(3) The Contractor shall be responsible for maintaining and ensuring continued compatibility and interoperability with the Government's systems, infrastructure, and processes for the term of the contract. In the event of an unavoidable compatibility and interoperability issue, the Contractor shall be responsible for providing timely notification to the Government and shall be responsible for working with the Government to identify appropriate remedies and if applicable, work with the Government to facilitate a smooth and seamless transition to an alternative solution and/or provider.			X		X		
Banner	The Standard Mandatory DoD Notice and Consent Banner will be displayed at log on to all DoD information systems. Choose either banner a or b based on the character limitations imposed by the system. The formatting of these documents, to include the exact spacing between paragraphs, must be maintained. The banner shall be implemented as a click-through banner at logon (to the			X				

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL	Add'l info req'd
	extent permitted by the operating system), meaning it prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating "OK."							
Banner	a. [Use this banner for desktops, laptops, and other devices accommodating banners of 1300 characters.]			X				
Banner	You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.			X				
Banner	By using this IS (which includes any device attached to this IS), you consent to the following conditions:			X				
Banner	- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations			X				
Banner	- At any time, the USG may inspect and seize data stored on this IS			X				
Banner	- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.			X				
Banner	- This includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.			X				
Banner	- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.			X				
Banner	OK			X				

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL	Add’l info req’d
Banner	b. [For Blackberries and other PDAs/PEDs with severe character limitations:]			X				
Banner	I've read & consent to terms in IS user agreement.			X				
Continuous Monitoring	The Contractor will provide all reports required to be completed; including self- assessments required by the FedRAMP Continuous Monitoring Strategy Guide to the Agency’s designated security point of contact. In addition, the Government may request additional reports based on data required to be collected by FedRAMP’s continuous monitoring requirements. If requested, the Contractor will provide the report to the Government within 10 business days.			X			x	
Cybersecurity Compliance	The Contractor will ensure that its environment is compliant with the control standards of FISMA (Federal Information Security Management Act) 44 U.S.C. § 3541, et seq.) , NIST standards in FIPS 140-2, FIPS 180, FIPS 198-1, FIPS 199, FIPS 200, FIPS 201 and NIST Special Publications 800-53, 800-59, and 800-60 and with agency management directive DODI 8500.1. In addition the Contractor must provide the Government with any documentation it requires for its reporting requirements within 10 days of a request.			X				
Cybersecurity Compliance	The Contractor will ensure that the cloud environment fully complies or exceeds the security requirements for level ___in the DoD Cloud Security Model SRG. The Contractor will make the environment accessible for a DoD security team to evaluate the environment prior to the placement of any DoD data in the environment and allow for periodical security reviews of the environment during the performance of this contract.		X					
Data Breach and Incident Reporting/PIA	DFAR 252.239.700x		X					

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL	Add'l info req'd
Data Breach and Incident Reporting/PIA	The Contractor shall adopt and maintain administrative, technical, and physical safeguards and controls to protect and remedy data breaches, if any, of Government data. The Contractor will submit reports of cyber incidents through approved reporting mechanisms, as specified in CJCSM 6510.01B, Enclosure C, Section 4. The Contractor's existing notification mechanisms that are already in place to communicate between the Contractor and its customers for some or all classes of CND information may be used, as long as those mechanisms demonstrate a level of assurance, equivalent to the listed encrypted mechanisms, for the confidentiality and integrity of the information.		X				x	
Data Breach and Incident Reporting/PIA	The Contractor will apply the template format specified in CJCSM 6510.01B, Appendix B to Enclosure C, Section 1 – General Cyber Incident Report Format when reporting initial incidents by secure fax, telephonically, or by other electronic means. Initial reports may be incomplete. Reporting should balance the necessity of timely reporting (reports with critical information) versus complete reports (those with all blocks completed). Timely reporting is vital, and complete information should follow as details emerge.		X					
Data Breach and Incident Reporting/PIA	In addition to the above, if the incident concerns a breach of PII or a potential breach of PII, the Contractor will report to the contracting officer's designee within 60 minutes of the discovery of any data breach. The Contractor shall provide the Government with all information and cooperation necessary to enable compliance by the Contractor and/or the Government with data breach reporting and mitigation actions required by applicable law, regulation, policy, and this contract.		X					

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL	Add'l info req'd
Facility Inspections	The Contractor agrees to have an independent third party or other industry recognized firm, which has been approved by the Government conduct a security audit based on the Government's criteria at least once a year. The audit results and Contractor's plan for addressing or resolving of the audit results shall be shared with the Government within 20 days of the Contractor's receipt of the audit results. In addition, the Government reserves the right to inspect the facility to conduct its own audit or investigation.		X	X				
Indemnification	(1) The Contractor shall indemnify the Government and its officers, agents, and employees acting for the Government against any liability arising out of the performance of this contract, including costs and expenses, incurred as the result of the Contractor's unauthorized introduction of copyrighted material, information subject to a right of privacy, and any libelous or other unlawful matter into Government data. The Contractor agrees to waive any and all defenses that may be asserted for its benefit, including (without limitation) the Government Contractors Defense.			X				
Indemnification	(2) The Contractor shall indemnify the Government and its officers, agents, and employees acting for the Government against any liability arising out of the performance of this contract, including costs and expenses, incurred as the result of (i) the Contractor's unauthorized disclosure of trade secrets, copyrights, contractor bid or proposal information, source selection information, classified information, material marked "For Official Use Only", information subject to a right of privacy or publicity, personally identifiable information as defined in OMB Memorandum M-07-19 (July 12, 2006), or any record as defined in 5 U.S.C. § 552a; or (ii) the Contractor's unauthorized introduction of any libelous or other unlawful matter into Government data. The contractor			X				

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL	Add'l info req'd
	agrees to waive any and all defenses that may be asserted for its benefit, including without limitation the Government Contractors Defense.							
Indemnification	(3) In the event of any claim or suit against the Government on account of any alleged unauthorized disclosure or introduction of data or information arising out of the performance of this contract or services performed under this contract, the Contractor shall furnish to the Government, when requested by the Contracting Officer, all evidence and information in the Contractor's possession pertaining to such claim or suit. Such evidence and information shall be furnished at the expense of the Contractor; provided, however, that an equitable adjustment shall be made under this clause, and the contract modified in writing accordingly, if the claim or suit is withdrawn, settled, or adjudicated in favor of the Government, and the basis for the claim or suit, regardless of outcome, was not due to any act or omission of the Contractor.			X				
Indemnification	(4) The provisions of this paragraph do not apply unless the Government provides notice to the Contractor as soon as practicable of any claim or suit, affords the Contractor an opportunity under applicable laws, rules, or regulations to participate in the defense of the claim or suit, and obtains the Contractor's consent to the settlement of any claim or suit other than as required by final decree of a court of competent jurisdiction; and these provisions do not apply to any libelous or other unlawful matter contained in such data furnished to the Contractor by the Government and incorporated in data to which this clause applies. Further, this indemnity shall not apply to—			X				

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL	Add'l info req'd
Indemnification	a. A disclosure or inclusion of data or information upon specific written instructions of the Contracting Officer directing the disclosure or inclusion of such information or data;			X				
Indemnification	b. A third-party claim that is unreasonably settled without the consent of the Contractor, unless required by final decree of a court of competent jurisdiction.			X				
Insurance	(1) The Contractor shall provide and maintain insurance, to include cybersecurity insurance, throughout the performance of this contract, as specified in the Schedule or elsewhere in the contract.			X				
Insurance	(2) Before commencing performance under this contract, the Contractor shall provide proof of insurance to the Contracting Officer. The Contractor shall resubmit the proof of insurance within 30 days of notification of any material change that occurs during the performance of the contract.			X				X
Insurance	(3) The Contractor shall insert the substance of this clause, including this paragraph (c), in subcontracts under this contract that require work with or in support of storage and retrieval of electronic/digital government data and shall require subcontractors to provide and maintain the insurance required in the Schedule or elsewhere in the contract. The Contractor shall maintain a copy of all subcontractors' proofs of required insurance and shall make copies available to the Contracting Officer upon request.			X				
Law Enforcement	(1) The Contractor shall record all physical access to the cloud storage facilities and all logical access to the government data as specified in the Schedule. This may include the entrant's name, role, purpose, account identification, entry and exit time. Such records shall be provided to the Contracting Officer or designee in			X				

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL	Add'l info req'd
	accordance with the Schedule or upon request to comply with federal authorities.							
Law Enforcement	(2) As specified by the Contracting Officer, the Contractor shall provide immediate access to all Government data and Government-related data impacting Government data for review, scan, or conduct of a forensic evaluation and physical access to any contractor facility with Government data. If the Government data is co-located with the non-Government data, the Contractor shall isolate the Government data into an environment where it may be reviewed, scanned, or forensically evaluated in a secure space with access limited to authorized Government personnel identified by the Contracting Officer, and without the Contractor's involvement.			X				
Location of Data	(1) The Contractor shall maintain all data within the United States, which means the 50 States, the District of Columbia, and outlying areas.		X					
Location of Data	(2) The Contractor shall provide the Government with a list of the physical locations which may contain government data within 20 days with updates on a quarterly basis.		X				X	
Maintenance	The Contractor shall be responsible for all patching and vulnerability management (PVM) of software and other systems' components supporting services provided under this agreement so as to prevent proactively the exploitation of IT vulnerabilities that may exist within the Contractor's operating environment. Such patching and vulnerability management shall meet the requirements and recommendations of NIST SP 800-40, as amended, with special emphasis on assuring that the vendor's PVM systems and programs apply standardized configurations with automated continuous monitoring of the same to assess and mitigate risks associated with known and unknown IT			X		X		

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL	Add'l info req'd
	vulnerabilities in the Contractor's operating environment. Furthermore, the Contractor shall apply standardized and automated acceptable versioning control systems that use a centralized model to capture, store, and authorize all software development control functions on a shared device that is accessible to all developers authorized to revise software supporting the services provided under this agreement. Such versioning control systems shall be configured and maintained so as to assure all software products deployed in the Contractor's operating environment and serving the Government are compatible with existing systems and architecture of the Government.							
Misuse of Government Data and Metadata	(1) The Contractor shall not access, use, or disclose Government data unless specifically authorized by the terms of this contract or a task order issued hereunder. If authorized by the terms of this contract or a task order issued hereunder, any access to, or use or disclosure of, Government data shall only be for purposes specified in this contract or task order. Contractor shall ensure that each of its employees and representatives, and any others (e.g., subcontractor employees) performing duties hereunder, shall, prior to obtaining access to any Government data, sign a contract or task order specific nondisclosure agreement.	X	X					
Misuse of Government Data and Metadata	(2) The Contractor shall use Government-related data only to manage the operational environment that supports the government data and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer.	X	X					
Misuse of Government Data and Metadata	(3) A breach of the obligations or restrictions set forth in (b)(1) and (b)(2) may subject the Contractor to criminal, civil, administrative, and contractual actions in law and equity for	X						

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL	Add'l info req'd
	penalties, damages, and any other appropriate remedies by any party adversely affected by the breach.							
Non-Disclosure Agreements	See number 6, Organizational Conflict of Interest. Ensure that all contractors sign an NDA.			X				
Notification	The Contractor shall notify the Government within 60 minutes of any warrants, seizures, or subpoenas it receives, including those from another Federal Agency that could result in the loss or unauthorized disclosure of any Government data. The Contractor shall cooperate with the Government to take all measures to protect Government data from any loss or unauthorized disclosure that might reasonably result from the execution of any such warrant, seizure, subpoena, or similar legal process.	X						X
Personnel Access	The Contactor will require all employees who will have access to government data, the architecture that supports government data, or any physical or logical devices/code to pass the appropriate background investigation required by the Government in compliance with HSPD -12. At a minimum, all Contractor employees with access to the government data, the architecture that supports government data, or any physical or logical devices/code will pass a NACI investigation and be a US person as defined in Executive Order 12333.		X[13]		X			
Physical Access	(1) The Contractor shall record all physical access to the cloud storage facilities and all logical access to the government data as specified in the Schedule. This may include the entrant's name, role, purpose, account		X				x	

[13] Referenced in existing clause.

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL	Add'l info req'd
	identification, entry and exit time. Such records shall be provided to the Contracting Officer or designee in accordance with the Schedule or upon request to comply with federal authorities.							
Physical Access	(2) As specified by the Contracting Officer, the Contractor shall provide immediate access to all Government data and Government-related data impacting Government data for review, scan, or conduct of a forensic evaluation and physical access to any contractor facility with Government data. If the Government data is co-located with the non-Government data, the Contractor shall isolate the Government data into an environment where it may be reviewed, scanned, or forensically evaluated in a secure space with access limited to authorized Government personnel identified by the Contracting Officer, and without the Contractor's involvement.		X					
Records	(1) The Contractor shall provide the Contracting Officer all Government data and Government-related data in the format specified in the Schedule or as directed by the Contracting Officer.	X					x	
Records	(2) The Contractor shall dispose of Government data and Government-related data in accordance with the Schedule and provide the confirmation of disposition to the Contracting Officer in accordance with contract closeout procedures.	X						
Records	(3) The Contracting Officer may at any time issue a hold notification in writing to the Contractor. At such time, the Contractor may not dispose of any Government data or Government-related data described in the hold notification until such time as the Contractor is notified in writing by the Contracting Officer, and shall preserve all such data in accordance with agency instructions.			X				

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL	Add’l info req’d
Records	(4) The Contractor shall provide the Contracting Officer within 10 business days of receipt of any requests from a third party for Government-related data.			X				
Records	(5) When the Government is using a Contractor’s software, the Contractor shall provide the agency with access and the ability to search, retrieve, and produce Government data in a standard commercial format.			X				
Spillage	(1) Upon written notification by the Government of a spillage, the Contractor shall coordinate immediately with the responsible Government official to correct the spillage in compliance with agency-specific instructions.	X						
Spillage	(2) If the Contractor incurs additional cost to correct the spillage, or the effort to correct the spillage causes a delay in the performance of any part of the work under this contract, and such costs or delays were not caused by any act or omission of the Contractor, an equitable adjustment shall be made under this clause and the contract modified in writing accordingly.	X						
Spillage	(3) No request by the Contractor for an equitable adjustment to the contract under this clause shall be allowed, unless the Contractor has given a written notice thereof within 30 days after the notification prescribed in paragraph (a) of this clause.	X						
Spillage	(4) No request by the Contractor for an equitable adjustment to the contract due to a spillage shall be allowed if made after final payment under this contract.	X						
Spillage	(5) Any spill of data by the Contractor into the environment hosting Government Data, will be immediately reported to the Government POC (insert POC) and the Contractor will follow the Government's instructions to clean up the spill at the Contractor's expense.	X						

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL	Add'l info req'd
Supply Chain	(1) Supply Chain Risk Management (SCRM) Plan. The offeror shall submit a SCRM plan as part of its technical proposal. The SCRM plan shall describe the offeror's approach to SCRM and demonstrate how the offeror's approach will reduce and mitigate supply chain risks. The SCRM plan shall address:			X				
Supply Chain	a. System Security Engineering. The SCRM plan shall describe the offeror's use of system security engineering processes in specifying and designing a system that is protected against external threats and against hardware and software vulnerabilities.			X				
Supply Chain	b. Criticality Analysis. The SCRM plan shall include the criticality analysis (CA) process used by the offeror to determine Mission Critical Functions and the protection techniques (countermeasures and sub-countermeasures) used to achieve system protection and mission effectiveness. The CA shall describe the offeror's supply chain for all critical hardware and software components (and material included in products), key suppliers, and include proof of company ownership and location (on-shore or off-shore) for key suppliers and component manufacturers. The CA shall identify critical functions and components (hardware, software, and firmware) in accordance with both DoDI 5200.44 "Protection of Mission critical Functions to Achieve Trusted Systems and Networks (TSN)". Criticality levels that support the CA are defined in the document "Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, "program Protection Plan Outline and Guidance," July 18, 2011.			X				

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL	Add'l info req'd
Supply Chain	c. SCRM Security Controls. The SCRM plan shall describe the offeror's strategy for implementing of SCRM security requirements throughout the life of the contract. The SCRM plan shall address the security controls (at a minimum SA-12) described in National Institute of Standards & Technology (NIST) Special Publication 800-53 Revision 4 (current version), Recommended Security Controls for Federal Information Systems and Organizations (http://csrc.nist.gov/publications/PubsSPs.html), and should be tailored in scope to the effort and the specific unclassified DoD information.			X				
Supply Chain	d. Delivery Mechanisms. The SCRM plan shall describe the offeror's physical and logical delivery mechanisms to protect against unauthorized access, exposure of system components, information misuse, unauthorized modification, or redirection;			X				
Supply Chain	e. Operational and Disposal Processes. The SCRM plan shall describe the offeror's operational processes (during maintenance, upgrade, patching, element replacement, or other sustainment activities) and disposal processes that limit opportunities to knowledge exposure, data release, or system compromise.			X				
Supply Chain	f. SCRM Training/Awareness Program.			X				
Supply Chain	(2) Contractor-Manufacturer Relationship. The SCRM plan shall identify the relationship between the offeror and the manufacturer as one of the following: (1) OEM; (2) authorized reseller; (3) authorized partner/distributor; or (4) unknown/unidentified source.			X				
Supply Chain	(3) Malicious Code Warranty. The SCRM plan shall include the offeror's expressed warranty that the software shall be free from all computer viruses, worms, time-outs, time			X				

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL	Add'l info req'd
	bombs, back doors, disabling devices and other harmful or malicious code intended to or which may damage, disrupt, inconvenience or permit access to the software user's or another's software, hardware, networks, data or information.							
Supply Chain	(4) Subcontracts. The Offeror shall incorporate the substance of this clause in subcontracts at all tiers where a subcontractor provides personnel, components or processes identified as either a critical component or its supporting infrastructure. All subcontractors providing critical components or services shall be identified and required to provide all necessary information to complete the SCRM Plan in association with the Offeror.			X				
Supply Chain	(5) SCRM Plan Submission & Review. The SCRM plan and supporting documents shall be submitted to the contracting officer as part of the offeror's technical proposal. All SCRM plans and appropriately marked related information will be treated as proprietary information by the Government and handled as Controlled Unclassified Information pursuant to Executive Order 13556 and shall be used solely for the purposes of managing risk to Government Functions. The government shall review the offeror's SCRM plan to determine whether the SCRM plan demonstrates an acceptable methodology for managing supply chain threats/risks. The SCRM plan review shall consider the offeror's SCRM approach for: (1) System Security Engineering; (2) Criticality Analysis; (3) SCRM Security Controls; (4) Delivery Mechanisms; (5) Operational and Disposal Processes; and (5) SCRM Training/Program Awareness. The SCRM plan must be deemed acceptable by the contracting officer in order for the offeror to be eligible for award. The offeror's failure to submit an acceptable SCRM			X				

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL	Add’l info req’d
	plan may result in the offeror being eliminated from further consideration for contract award.							
Supply Chain	(6) Material Term of the Contract. Failure by the offeror to submit an acceptable SCRM Plan with its proposal may result in the offeror’s exclusion from award. Failure by the Contractor to execute, maintain and distribute a current SCRM Plan for review by the Government in accordance with the terms of the contract shall constitute a material breach of the contract and may result in termination for default or cause.			X				
Terms of Service	Use FAR Clause: 52.212-4(u): The following shall supersede any language in the Contractor’s commercial terms of service:		X					
Terms of Service	(1) Confidentiality. The Government, to the extent permitted by law and regulation, will safeguard and treat information obtained pursuant to the Contractor’s disclosure as confidential where the information has been marked “confidential” or “proprietary” by the company. To the extent permitted by law and regulation, such information will not be released by the Government to the public pursuant to a Freedom of Information Act request, 5 U.S.C. § 552, without prior notification to the Contractor. The Government may transfer documents and information provided by the Contractor to any department or agency within the Executive Branch if the information relates to matters within the organization’s jurisdiction.		X					
Terms of Service	(2) Disputes and governing law. Any and all other terms or conditions notwithstanding, disputes arising under or relating to this contract or agreement are subject exclusively to Federal law, particularly the Contract Disputes Act of 1978, as amended (41 U.S.C. §§ 7101-7109) (the Act) and the provisions of 48 CFR subpart 33.2. Except as provided in			X				

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL	Add'l info req'd
	the Act, all disputes arising under or relating to this contract shall be resolved under the clause set forth at 48 CFR 52.233-1.							
Terms of Service	(3) Other legal matters. Any and all other terms or conditions notwithstanding, legal actions in which the Government is a party that do not arise under or relate to this contract or agreement shall be prosecuted under applicable Federal law in the appropriate Federal venue.			X				
Terms of Service	(4) Endorsement. The Contractor may not use the name, seal, logo or other readily identifiable indicia of any Government agency or organization in such a way that may be construed as advertising or endorsement by the Government of the Contractor. The Contractor may include within a list or display of the Contractor's customers for the purposes of advertising or publicity the names, seals, logos or other indicia of Government agencies and organizations that have entered into contracts with the Contractor. However, it must not be stated or implied that the Government in any way recommends or endorses the products or services of the Contractor			X				
Terms of Service	(5) Indemnification and renewal. Any other terms or conditions notwithstanding, this contract or agreement shall not and does not require the Government to (i) indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability, which would violate the Anti-Deficiency Act (31 U.S.C. § 1341) (ADA), or (ii) automatically renew this contract or agreement at any time in the future, which would violate the ADA. Any such provisions set forth in this contract or agreement are unenforceable against the Government.	X[14]						

[14] Referenced in another FAR Clause.

Description	Contract Language	DFAR	IR	PWS	SRG	SLA	CDRL	Add'l info req'd
Use of Subcontractors	The Contractor shall retain operational configuration and control of data repository systems used to process and store government data to include any or remote work. The Contractor shall not subcontract the operational configuration and control of any government data.			X				