	subject to JCIDS and should be handled as specifically provided for by the Vice Chairman of the Joint Chiefs of Staff, in consultation with Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) and each service acquisition executive. In some cases, the Joint Staff should determine if joint equities are involved and execute an expedited joint validation process if necessary. 1. <u>Validate Strategic Alignment:</u> • For applications, PMs should document alignment with the National Defense Strategy and DoD Digital Modernization Strategy in the Capability Need Statement (CNS). • For embedded software, PMs should cite documentation associated with the overarching program for which the software integrates in the CNS as evidence of alignment with the National Defense Strategy and DoD Digital Modernization Strategy. 2. <u>Validate Investment Decision Alignment:</u> Using the CNS, User Agreement, acquisition strategy, and test strategy as	strategy should include recurring assessment of the supply chain, development environment, processes and tools, continuous automated cybersecurity test, and operational evaluation. It must also identify cybersecurity testing needed to validate its mitigation. 2. <u>Identify Level of Risk Acceptance and Associated Security Controls:</u> Depending on the architecture, the PM may require an ATO or an "assess only" approval. In the case of an "assess only", the software must be running on an approved platform. Use of platforms with approved DevSecOps capabilities and a continuous ATO is encouraged. The PM should work with their security team to identify the controls needed not already inherited by the platform. ***<u>Data</u>*** Data requirements should be discussed throughout the Planning Phase and addressed in the CNS. This should include consideration for APIs and management of federated data catalog artifacts. For software, it is critical that data rights account for the full scope of artifacts	strategy that includes records management requirements per DoD 5015.02-STD.	acquisition value assessment conducted on an iterative basis in alignment with the software release plan. PIR is further discussed in Section 5, Sustaining Digital Capabilities.

	a baseline, the PM should develop a cost estimate. The cost estimate should fall within the bounds of identified budget lines and in alignment with application rationalization analysis and IT portfolio decisions. Software investments should not duplicate existing capability. PMs should leverage existing capability to the greatest extent practical.	needed to transition the capability.		
Defense Business Systems	**Capability Needs Identification** ***CCA Compliance*** Validate Strategic Alignment: a) PMs should document alignment with the National Defense Strategy and DoD Digital Modernization Strategy in the description of the business problem or opportunity. b) PMs should align to the Business Enterprise Architecture. c) PMs should use DITPR/SITR data to assess existing capabilities and identify organizations with similar capability needs. d) PMs should leverage outcomes/decisions from the Defense Business Council and associated IT portfolio management working groups to validate alignment to	**Solutions Analysis** ***CCA Compliance*** Investment Registration in DITIP: PMs should register the DBS as an investment within DITIP in accordance with the DoD Annual Budget Guidance prior to receiving the Functional Requirements Authority to Proceed (ATP). ***Data*** Data requirements should be discussed throughout the Solutions Analysis phase and addressed in the Acquisition Strategy and Capability Implementation Plan. This should include consideration for APIs and management of federated data catalog artifacts. For software, it is critical that data rights account for the full	**Functional Requirements and Acquisition Planning** PMs develop functional requirements to describe how the business system will achieve future business processes. PMs submit required documentation in the Capability Implementation Plan to progress to the Acquisition ATP. PMs participate in the annual OSD investment management process and provide/update the following information/data sources to receive an approved investment decision memorandum to draw down funds in the upcoming fiscal year. 1. DBS must be registered within DITIP and reflect Title 10 Section 2222(g) compliance 2. DBS has an updated and complete record within the	**Acquisition, Testing, and Deployment and Capability Support** ***CCA Compliance*** 1. Update Acquisition in DITPR/SITR: PMs should continue to update DITPR/SITR with required data fields to reflect the current status of the solution. DITPR/SITR information will be used to support of DBC quarterly reviews, future budget certification, and the issuance of annual investment decision memorandums. 2. Participate in the Information Technology Purchase Request Process (ITPR) using IT PAT: PMs aligned to Fourth Estate organizations must request DoD CIO approval for

should list the applicable policies and standards on the task order or delivery order. When citing policy, a best practice is to add the verbiage “or current version” to the policy referenced so that the requirements reflect the most current policy statements.

- Acquired cloud service provider infrastructure connected to the DoDIN is subject to DoDIN security requirements and standards. (Reference Joint Publication (JP) 3-12 (R): Cyberspace Operations, February 5, 2013)
- Classified contractor infrastructure must follow the National Industrial Security Program as established by Executive Order 12829. (Reference Executive Order 12829 - National Industrial Security Program, January 8, 1993)
- Cloud service offering must comply with the DoD CC SRG. (Reference current version of the DoD CC SRG)
- Contractor must provide the ability for actions to be logged to an immutable destination within the cloud offering. Such logs must provide an audit trail that supports the functions outlined in DoD Instruction 8530.01. (Reference DoD Instruction 8530.01, Cybersecurity Activities Support to DoD Information Network Operations, July 25, 2017)
- Cyber incidents and breaches must be reported in accordance with DFARS 252.239-7010.
- DoD operators and/or auditors are authorized to verify compliance with standards and policies to include FedRAMP, the DoD CC SRG, and other applicable policies.
- Infrastructure must be accredited in accordance with the applicable DD Form 254 on the contract/task order/delivery order.
- Classified and unclassified server and media destruction is to be done pursuant to DoD Directive 5220.22-M. (Reference DoD Directive 5220.22-M, National Industrial Security Program Operating Manual, February 28, 2006)
- Classified and unclassified server and media deletion is to be done pursuant to NIST SP 800-88 (0.17).
- Physical isolation must be compliant with National Security Telecommunications and Information Systems Security Advisory Memoranda (NSTISSAM) Level. (Reference NSTISSAM Level I: Compromising Emanations Laboratory Test Standard)
- Logical separation of unclassified infrastructure and encryption with FIPS 140-2 approved cryptographic implementations is required for data both at rest and in transit. Encryption pursuant to CNSSP 15 is required for unclassified NSS data both at rest and in transit. (Reference NSTISSAM Level I: Compromising Emanations Laboratory Test Standard)
- Logical separation within classified infrastructure requires encryption with NSA approved cryptography for data both at rest and in transit pursuant to CNSSP 15. (Reference Committee on National Security Systems (CNSS) Policy 15, Use of Public Standards for Secure Information Sharing, October 20, 2016)
- Contractor must support management of encryption keys internally and by the Government pursuant to CNSSP 30. (Reference D.13 CNSS Policy 30, Cryptographic Key Protection, December 28, 2017)
- Unclassified authentication requires multi-factor authentication such as DoD PKI as defined in DoD Instruction 8520.03. (Reference DoD Instruction 8520.03, Identity Authentication for Information Systems, July 27, 2017)
- Access to classified infrastructure requires DoD PKI-based authentication at the appropriate classification level pursuant to DoD Instruction 8520.03 and CNSSP 25. (Reference DoD Instruction 8520.03, Identity Authentication for Information Systems, July 27, 2017, and CNSSP 25, National Policy for Public Key Infrastructure in National Security Systems, December 11, 2017)

- Highly granular access control configuration is required for compliance with technical policies as defined in NIST SP 800-63. (Reference NIST SP 800-63: Digital Identity Guidelines, Revision 3, June 2017)
- Secure data transfer capabilities provided must meet DoD's requirements as described in the 2018 Raise the Bar Cross Domain Solution Design and Implementation Requirements document. The secure data transfer capabilities will be assessed in accordance with DoD Instruction 8540.01 and CNSSI 1253F Attachment 3, Cross Domain Solution (CDS) Overlay, September 2013.
- Account management, authentication, and authorization services must be isolated from those used by other customers with the ability to prevent access to these services from the Internet and any other network not specifically authorized.
- Any traffic of data above IIL-2 moving between the DoDIN and any Contractor Point of Presence (POP) that bypasses DoD's CAP requires approval of the DoD CIO or their designated representative(s).
- The cloud service provider must support both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) network addressing.
- The cloud service provider and PM will coordinate forensic and compliance audits pursuant to NISTIR 8006l0. (Reference NISTIR 8006: Cloud Computing Forensic Science Challenges, June 30, 2014)
- Records must be managed on behalf of and be available to the PM in accordance with the Federal Records Act. Contractors are responsible for following records management laws when they act on behalf of the government. (Reference Title 44 U.S.C., Chapter 31: Records Management by Federal Agencies)
- Contractor is to support DoD's role in providing cybersecurity support services in accordance with DoD CIO CSSP Memorandum. (DoD CIO Memorandum, Department of Defense Cybersecurity Activities Performed for Cloud Service Offerings, November 15, 2017)
- Ensure unauthorized access does not occur. (References: CNSS Instruction 1253F Attachment 5: Classified Information Overlay , May 9, 2014; DoD Directive 8100.02: Use of Commercial Wireless Devices, Services and Technologies in the Department of Defense Global Information Grid, April 23, 2007; FIPS PUB 140-2: Security Requirements for Cryptographic Modules, December 3, 2002; OMB Circular No. A-130: Managing Information as a Strategic Resource, July 28, 2016; CNSS Policy 11: Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products, June 1, 2013)
- Contractor ensures cloud service provider support to Government cybersecurity test and evaluation including access to system logs, packet capture, and other cloud service offering information to support problem resolution, test results, and test reporting. (Reference: DoD Cybersecurity T&E Guidebook v2, April 2018; Addendum: Cybersecurity T&E of DoD Systems Hosted on Commercial Cloud Service Offerings)
- Contractor provides a testing environment that emulates the operational environment to support test and evaluation and the ability to connect a DoD cyber test range emulation of DoDIN infrastructure to the test environment.

5) Plan for Appropriate Tests

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

- Verify mechanisms to ensure Government data is protected from unauthorized disclosure and remains under Government control

- Verify configuration and protections of external and internal data flows between applications, containers, virtual devices, virtual machines, cloud service offering infrastructure, and DoD infrastructure
- Verify data at rest encryption on cloud service provider infrastructure
- Verify data leak protection between applications, virtual machines, or physical infrastructure

To facilitate security testing, the contract should address items such as cloud service provider support to Government testing and access to test results if previous cloud service offering testing was performed. Examples of items to consider when developing the contract to facilitate cloud service provider support to DoD test and evaluation include the following:

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

6.4.2 Data

Data Ownership

Another critical requirement is ensuring that the agency acquiring cloud services retains ownership of the data it acquires (commercial/public or Governmental asset), generates, and 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 cloud service provider if it is not satisfied with the services it receives. This point must always be made clear with the cloud service provider prior to the acquisition and specified in writing in the final contract. Another point of emphasis is that data relationships should also be portable. An example of this need is for records management – records depend on data structures and their relationships.

Data Breach

Ownership rights are especially important to negotiate beforehand to address potential data breaches. It is a best practice to ensure that the cloud service provider 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 cloud service providers indemnify Federal Agencies if a breach should occur and the cloud service provider should be required

to provide adequate capital and/or insurance to support their indemnity. In instances where expected standards are not met, then the cloud service provider must be required to assume the liability if an incident occurs directly related to the lack of compliance."

Data Jurisdiction

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

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

The vendor shall identify all data centers that the data at rest or data backup will reside. All data centers will be guaranteed to reside within defined boundary / country / jurisdiction.
The vendor shall provide a Wide Area Network (WAN), with a minimum of # data center facilities at # different geographic locations with at least # Internet Exchange Points (IXP) for each price offering. The vendor shall provide Internet bandwidth at the minimum of # GB.

6.4.3 Cost

Cost Trade-Off

Is there a reasonable cost trade-off between leveraging a cloud service and building a capability?

Adopting cloud services is not solely about cost efficiencies. The pace of innovation through cloud exceeds what is possible by a single enterprise alone and the global reach of cloud infrastructure supports the faster delivery of data. However, cost must be considered prior to pursuing cloud services to ensure not only an appropriate trade-off between cost and operational benefit, but an informed approach in shaping the acquisition strategy.

To determine cost trade-off, PMs oftentimes conduct business case analysis (BCA) or something similar. The BCA is not a requirements validation process. It is intended to ensure a consistent approach to IT investment analysis. BCA analysis should coincide with an organization's portfolio management processes, which drive alignment of investments with the vision and priorities of the organization. The BCA or similar analysis should achieve the following:

- Facilitate comparison of alternatives
- Define expected costs, benefits, operational impacts, and risk

The major components of a BCA or similar analysis include the following:

- Cost and economic viability
- Requirement satisfaction/completeness
- Operational benefit (qualitative)
- Risk assessment
- Recommendations based on a balance between cost effectiveness and operational benefit
- Funding type and sources

PMs should submit their BCA or similar analysis as part of their acquisition planning to the decision authorities for their selected acquisition pathway.

General Cost Considerations

What are cost considerations in determining contract type to obtain the most advantage from cloud usage billing?

Table 7 below outlines several areas to consider when acquiring cloud services. It is critical to understand how these services are deployed and operated to avoid paying for services not utilized.

Table 7: Cost Drivers for Cloud Services

Cost Driver	Consideration
Over-Provisioning	Over-provisioning is when demand for an application is overestimated. Cloud service providers make it easy to max out and the costs become inflated. Although servers can be scaled back, this is potentially a slow process. Ways to decrease costs include the following: • Ensure virtual instances are shut down when not in use • Understand uptime requirements and scheduling • Monitor usage
Under-Provisioning	Under-provisioning is when demand is underestimated. It is easier to detect and fix since it means the cloud service's performance is not acceptable.
Spin It Up, Then Forget It	Having too many administrators in the cloud is costly since they do not always communicate with each other and may spin up server instances for a particular purpose that are never used. Costs can be saved, and security improved by turning off resources that are no longer needed.
Storage Choices	Many cloud service providers offer different tiers of storage pricing based on data accessibility. Standard storage is frequently accessible, yet most expensive. A semi-accessible tier is for data that needs to be kept but rarely accessed. Organizations should consider which tier structure they need for specific data. Since storage grows and never shrinks, storage consumption should be actively managed by moving data to lower cost services when they are no longer in constant use, caching and deleting files as appropriate.
Free (with Strings Attached)	The "free tier" is billable if thresholds are exceeded, and this happens frequently without the administrator realizing it. Some free cloud service offerings also have an expiration date after which the full billing rate applies.
Appliance Charges	Some commercial cloud service providers offer a menu of different virtual network and server instances that can be "rented" (e.g., load balancers, VPN concentrators, and databases). Unless the exact frequency of usage is known, choosing a size and payment model can be challenging and will lead to higher than necessary costs.
Free To Enter, Pay To Leave	It is never a good idea to shop for a commercial cloud service provider when IT needs are high, and timelines are tight. It may lead to selection of a provider who is costly. Data migrated to the cloud for free may be costly to migrate out.
Troubleshooting Complexities	Troubleshooting is typically an overlooked cost that becomes more time consuming and expensive over time. The root cause of complex technical issues is challenging to resolve because there is often no visibility into a cloud and in-house staff must work with the service provider to resolve issues.
Software as a Service (SaaS)	SaaS nearly always carries a perpetual, per-user license (paid monthly on an annual or multi-year term). Hidden costs include the following: • Customization – To lower costs, SaaS should be used as designed. Customization leads to unanticipated development and maintenance costs.

	• Integration and Testing – SaaS typically integrates with in-house applications, data stores, and/or other SaaS services. A best practice is to define an integration architecture with as simple a business process as possible, then test the integrated services to understand capabilities and security features. • Sprawl – Access to SaaS must be carefully monitored. Most vendors have volume pricing for SaaS, meaning the more units purchased, the less per unit cost.
Not Activating Cloud Economics for Applications	Not every application fits with a pay-per-use platform. PMs should consider the most appropriate pricing model and include the following: • Elastic Scale – Application increases or decreases its resource consumption based upon usage. • Transient – Application can be parked or shut off when not in use (e.g., batch work, high performance computing, seasonal apps).
Data Consumption	Data consumption is the biggest cost driver. Cloud-based applications should be regularly optimized for better database performance (such as storage architecture and query optimization) or they may use unnecessary resources, increasing costs.

DoD-Specific Cost Considerations

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. This form of billing is widely used in the private sector but not common among Government customers. Acquiring cloud services within the constraints of the FAR and other DoD-specific regulations is difficult because Government/DoD systems were not designed to accommodate the variable usage and quick-pay cycles that are the hallmark of commercial cloud computing models.

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

To mitigate this disadvantage, PMs should consider the use of Time and Materials (T&M) type contracts, and/or flexibilities within the FAR. T&M contracts allow for cloud resource units to be treated as labor hour rates (fixed unit price). Flexibilities that exist within the FAR include the following approaches:

<u>Approach 1 – Optional CLIN Not to Exceed (NTE)</u>

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

Approach 2 – Drawdown Accounts

Drawdown Model A: Government Monitors

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

Pros: Allows customers to realize elasticity and flexibility benefits of cloud services.
Cons: Burdensome bookkeeping for the contracting officer or vendor as usage can be unpredictable.

Approach 3 – Subscription Based

Under the subscription model, 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 Firm Fixed Price contract for cloud services receives the benefit of knowing each monthly invoice amount. However, 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 metered billing.

Pros: This option works well if the hosting options are consistent throughout the life of the contract. It is low risk due to a certainty of forecasted utilization and is relatively simple to execute.
Cons: Government typically adds a buffer which leaves money on the table. The contracting officer obligates $100k per month for what should be $60k.

Table 8: Difference in Funding Cloud Considerations

Private Enterprise	Public Enterprise
Pays for cloud with "consumption-based" model using metered billing	Is constrained by budgeting and spending regulations and cannot utilize true "metered" services
Has flexible budgeting cycles and methods	Has restricted budgeting based upon fiscal year
Utilizes business-to-business contracts that allow for front-loading and cost overruns	Cannot incur obligations in excess of contract funding
Has the 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

Licensing

An additional cost consideration is licensing. Is the system or application licensed per virtual machine, per core, or for total infrastructure footprint?

This can have massive cost implications. If the licensing model requires that all available resources be considered even if not allocated to the client, licensing costs will increase if migrated to a public-cloud platform. Similarly, if the application licensing is based per core and the cloud provider does not offer the ability to configure the cloud environment per core, this will have an adverse impact on licensing cost. PMs should absolutely ensure that all Cloud Licensing Fees are known and spelled out in the beginning of the contract.

6.4.4 Contracting

Acquisition Pathway

Many cloud services requirements can be and should be acquired using the acquisition of services pathway per DoDI 5000.74. Cloud service considerations for each step in the services pathway is described in Figure 2.

Figure 2: Services Pathway for Cloud Services

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

Choosing a Cloud Service Model and Contract Type

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

PMs should consider the service models required and then determine the attributes of those service models. PMs should consider IaaS and PaaS together, and SaaS on its own. The attribute to consider under IaaS or PaaS is whether or not IT professional services are needed in support of the service model. For SaaS, attributes to consider include seats and usage, but IT professional services are still an important consideration depending on the service. This information sets up a framework for an appropriate discussion on cloud service models and contract types. An additional consideration for KOs is to understand technical responsibility and writing that responsibility into the contract. In IaaS or PaaS, the agency brings its own licenses and may or may not update them depending on funding. In the SaaS model, the cloud servicer provider is responsible for the application layer all the way down the stack. Also, in the SaaS model or subscription model, the agency needs to budget for the service.

In 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, an FFP contract should be used. Contract risk should be relatively low and predictable within acceptable limits. The vendors and agency can reasonably agree on price. This does not come without risk as agencies can be charged for services not used or are charged more than expected (neither scenario takes advantage of pay for use promised by a cloud solution). In cases where agencies require support services, they should consider a T&M CLIN separate from the IaaS and PaaS FFP CLINs and identify their requirements for the CLIN. Agencies can avoid these risks by writing in broad CLINs, providing the customer with 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 contracting office (KO) buy-in as the FAR imposes limitations on T&M contracting. If an agency selects an FFP contract type for a SaaS procurement, KOs should allow for flexibility at the CLIN or task order level so cost savings can be realized.

Table 9: Service Model Contract Type Considerations

Model	FFP Considerations	T&M Considerations
IaaS PaaS	• Use when no professional services needed • Use when vendor and agency agree on price	• Use when support services required (should be separate from FFP order) • Identify support needs in CLINs
SaaS	• May be favored by agency KO • 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 KO buy-in

Choosing a Requirements Document Type

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

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

Many agencies use an 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 and the amount of memory and storage, 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, and the average number of pages viewed per visit are provided in an SOO.

Table 10: Requirements Document Type Benefits

Requirements Document Type	When to Use and Benefits
SOO	• States performance objectives and constraints (e.g., security or availability), but is not prescriptive on "how" the work should be accomplished • Allows vendor creativity in proposing solutions • Good to use when agency can provide usage statistics and has no preferred or mandated way of providing the service • Usually shorter than SOW or PWS
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
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 services, an SOO issued within an RFP should 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 cloud service provider, then this may be an optimum solution. Cloud service providers may respond with their full price list of available services, which the agency can pick and choose from at the task order level. Since this could be extremely difficult to evaluate and defend in a potential protest, the acquirer may want to use sample task orders as a means of level setting for purposes of evaluation.

The final selection of the SOO, SOW, or PWS is authorized by the ordering KO based on the characteristics of the acquisition. It is important for the PM to engage with their KO early in the process because decisions like these need to be made throughout acquisition planning. For example, an SOO may allow the vendor to provide more innovative solutions, but they are difficult to evaluate since cloud service provider offerings are often quite different. A PWS may be used at the high level with just the end state defined. This allows for innovative solutions to be proposed.

Choosing a Blanket Purchase Agreement (BPA)

BPAs are an important tool that can solve certain elaborate cloud service challenges. A BPA, governed by 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 IDIQ instrument with those contractors who are qualified sources of supply. A BPA is not a contract and does not obligate funds. A BPA simply establishes the terms and conditions and pricing under which a purchase would occur including contract types and clauses.

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

IDIQs can apply across a host of opportunities and should be considered as a viable procurement strategy. For example, the Army ACCENT multiple award IDIQ had many characteristics that fit a BPA procurement strategy such as recurring transition requirements. Army wanted a standard tool that preset all the base requirements for their estimated 10,000 applications that are to be migrated to the cloud. The contract requirements included IaaS, SaaS, and PaaS offerings and had offerors demonstrate a DISA-issued provisional authorization for award. It further included in scope all of 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 cloud service provider 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.

Incorporating Appropriate Contract Clauses

There are various clauses to consider for cloud services with the first being the Defense Federal Acquisition Regulation Supplement (DFARS), Subpart 239.76, Cloud Computing. This clause and related clauses require the following:

- The contractor shall maintain within the United States or outlying areas all Government data that is not physically located on DoD premises, unless the contractor receives written notification from the KO to use another location.
- The contractor shall provide the Government with a list of the physical locations which may contain Government data within 20 days. Updates are required on a quarterly basis.
- The U.S. Government restricts the transfer of sensitive or classified data (such as sensitive technology information and information that could potentially affect operational security) to locations outside of the control of U.S. companies or the U.S. Government.
- There are specific rules for the locations of data processing centers based on the IIL of the data:
  - IIL-2 and 4 must be hosted at locations in the U.S., U.S. territories, or on DoD premises per the Status of Forces Agreement (SOFA) unless the location is authorized by the AO.

- IIL-5 must be hosted at locations in the U.S., U.S. territories, or on DoD premises per SOFA.
- IIL-6 must be hosted at locations authorized for classified processing.

Other contract considerations include the following:

- Availability and Availability Reporting of Cloud Services
  - Service Interruption Reporting – The contractor must inform the Government of any interruption in the availability of the cloud service as required by the SLA.
  - Outage Estimate – Whenever there is an interruption in service, the contractor shall inform the Government of the estimated time that the system or data will be unavailable.
  - System Availability Requirements – The estimated timeframe for recovery of the service must be related to the FIPS 199 system categorization for the availability of the system, and if specified, the contractor shall meet the agreed upon service level and system availability requirements.
  - Testing – Cloud service providers may place limitations on certain types of security testing in the cloud service offering used by the Government. Programs should specify language in the request for proposal and contract to obtain the required test and evaluation support. Programs should also ensure the SLA includes metrics to demonstrate via testing that the cloud service provider is delivering the mission owner's required cybersecurity, survivability, and operational resilience capabilities.
  - Status Updates – The contractor shall provide regular updates to the Government on the status of returning the service to an operating state according to the agreed upon SLAs and system availability requirements.
- Protection of Government Data
  - Protection of Government data is required by the Federal Acquisition Regulations (FAR) procedures, guidance, and information (PGI).
  - Data ownership, licensing, delivery, and disposition instructions specific to the relevant types of Government data and Government-related data shall be part of the contract.
  - Appropriate limitations and requirements regarding contractor and third-party access to, and use and disclosure of, Government data and Government-related data shall be documented in the contract.
  - Contract should include appropriate requirements to support applicable testing, inspection, audit, investigation, or other similar authorized activities specific to the relevant types of Government data and Government-related data, or specific to the type of cloud services being acquired.
  - Contract should include appropriate requirements to support and cooperate with applicable system-wide search and access capabilities for inspections, audits, investigations, litigation, eDiscovery, FOIA requests, records management associated with the agency's retention schedules, and similar authorized activities.
  - Contract should include a requirement for the contractor to coordinate with the responsible Government official designated by the KO, in accordance with agency procedures, to respond to any spillage occurring in connection with the cloud services being provided.
  - Contract should include a requirement that the contractor 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 KO.
  - Contract should ensure access to Government data for law enforcement and other purposes.

  - Contract should ensure compliance with regulations for Government records management policies. PMs should consult the National Archives and Records Administration's "Records Management Language for Contracts" site for any applicable Federal records management requirements to include in the contract.
  - Contract should include provisions of rights retention for all data derived products and outcomes.
- SLAs
  - Contract should define service levels (SLAs added to SOO/PWS or standalone).
  - SLAs should clearly define the contract performance standards, how the contractor measures and reports the service performance, and the enforcement mechanisms for SLA compliance.
  - Contract should clearly specify whether there are any maintenance windows when service can be disrupted and notification procedures for planned and unplanned outages.
  - Contract should clearly define any monitoring and metering requirements the organization has for monitoring the performance of the cloud service provider, for capturing the organization's usage patterns, and for charging the organization's clients for services.
- Other Contract Clause Considerations
  - Contract should clearly define subcontracting rules.
  - Contract should ensure proper supply chain management.
  - Contract should include clear terms of services. Many cloud services have Terms of Service Agreements that contain clauses that the Government cannot accept. Common examples are below:
    - Confidentiality. This is a clause where the Government agrees not to release confidential information. However, the Government is subject to the Freedom of Information Act and must follow its procedures to release or protect commercial information.
    - Indemnification. Many Terms of Service Agreements contain an open ended indemnification clause where the Government will indemnify the cloud service provider against third party claims. This type of clause violates the Anti-Deficiency Act because the Government is committing to funds that have yet to be appropriated.
    - Governing Law. Many Terms of Service Agreements have the governing law for the agreement to be a specific state and have a venue for any disputes to be in that state's courts. As the Federal Government is not subject to state law, it can only be sued in Federal court.
    - Endorsement. Many Terms of Service Agreements have a clause where the cloud service provider may quote/cite the Government's use of its product as an endorsement or testimonial. The Government does not endorse commercial products or services.

Table 11: Other Contracting Considerations for PMs

Considerations	Description
Banner	• Banner language provides consent for the Department to view any content on the system without a warrant. • When acquiring SaaS, consider requiring the cloud service provider to display DoD's approved banner language prior to allowing user access to the system.
Direct Contractual Relationship	• Contractual liability to the Government only exists with the prime contractor. When the PM acquires a commercial service through an intermediary (e.g., system integrator, value added reseller), only the intermediary is accountable to the

	Government. This reduces the contractual liability to the cloud service provider acting as the subcontractor, but increases the risks to the Government.
Exit Strategy and Plan	• Consider developing an interoperable strategy to move systems/applications from one cloud service provider to another.
Indemnification	• Consider requiring the cloud service provider to indemnify the Government against lawsuits; this protects the Government when third parties sue the Government for a tort when the cloud service provider, not the Government, is liable.
Insurance	• Consider requiring a cloud service provider to use insurance services pay for any costs stemming from a breach of DoD data (e.g., PII or PHI) or to replace any damages to the DoD system, including credit monitoring.
Ownership Rights	• Consider if a third party will own any aspects of assets that are applied for service provisioning.
Training	• Consider whether a training and change management program is needed to optimize implementation of security and cyber defense changes.

Incorporating Financial Audit Clauses

For financial or non-financial systems or applications impacting internal controls relevant to multiple DoD financial audits, PMs should obtain annual System and Organization Control (SOC 1) Type II reports from cloud and data center hosting organizations and application service providers (ASP). In those instances, where only a single DoD audit is impacted, an alternate solution is the inclusion of a right to audit clause in the relevant service organization contract. PMs should work with their financial and contract personnel to determine if their cloud/data center hosting organization or ASP is affected and to ensure service organizations and relevant sub-service organizations submit SOC 1 Type II reports in accordance with joint-issued DoD CIO and Under Secretary of Defense (Comptroller) guidance, "System and Organization Control Report Requirement for Audit Impacting Cloud/Data Center Hosting Organizations and Application Service Providers."

6.4.5 Service Level Agreements (SLAs)

The SLA is a contract between a cloud service provider and a cloud service consumer that specifies, in measurable terms, what services and guarantees the cloud provider will provide. As more and more consumers migrate their internal services to cloud providers, a detailed and legal binding SLA between the parties should emerge as a key characteristic of this relationship. Due to the nature of cloud service offerings, continuous monitoring and proper risk management are necessary attributes to enforce SLAs. Other factors such as trust (with the cloud service provider) come into play, particularly for customers that outsource their critical data to a cloud service provider's operation. This complexity requires a sufficient amount of governance.

An SLA should be part of the contract and achieve the following:

- Define the service and service levels being provided
- Set performance characteristics
- Identify metrics and how they will be measured
- Identify guarantees and methods of redress
- Address federal computing and physical security requirements
- Address risk management

Table 12: Key Practices for Cloud Service SLAs

Key Practice	Activities
Roles and Responsibilities	• Specify roles and responsibilities of all parties with respect to the SLA and, at a minimum, include agency and cloud providers. • Define key terms, such as dates and performance.
Performance Measures and Verification Processes	• Define clear measures for performance by the contractor. Include which party is responsible for measuring performance. Examples of such measures include: – Level of service (e.g., service availability—duration the service is to be available to the agency) – Capacity and capability of cloud service (e.g., maximum number of users that can access the cloud at one time and ability of provider to expand services to more users) – Response time (e.g., how quickly cloud service provider systems process a transaction entered by the customer, response time for responding to service outages) • Specify how and when the agency has access to its own data and networks. This includes how data and networks are to be managed and maintained throughout the duration of the SLA and transitioned back to the agency in case of exit/termination of service. • Specify the following service management requirements: – How the cloud service provider will monitor performance and report results to the agency. – When and how the agency, via an audit, is to confirm performance of the cloud service provider. • Provide for disaster recovery and continuity of operations planning and testing, including how and when the cloud service provider is to report such failures and outages to the agency. In addition, include how the provider will remediate such situations and mitigate the risks of such problems from recurring. • Describe any applicable exception criteria when the cloud provider's performance measures do not apply (e.g., during scheduled maintenance or updates).
Security	• Specify metrics the cloud service provider must meet in order to show compliance with the agency's security performance requirements for protecting data (e.g., clearly define who has access to the data and the data protections in place). • Specify performance requirements and attributes defining how and when the cloud service provider is to notify the agency when security requirements are not being met (e.g., when there is a data breach). • Specify cloud service provider support for Government security verification of operational metrics and the performance metrics defined above.

The Exit Strategy

In some cases, cloud service providers offer a subscription-based service, which means PMs need to be clear on two key things. First, PMs need to know how frequently the SLA will be revised and how much warning will be received. Second, the SLA should clearly stipulate the terms and procedures for cancelling the partnership. These critical factors break down to include things like the secure erasure of any confidential business data in the care of the provider. While PMs want to look at a provider with a long-term partnership in mind, it is critical that the contract be fully aware of the obligations of both parties when it comes to terminating the partnership.

Standards 19086 Series – SLAs

The International Classification for Standards (ICS) is a convention managed by the International Organization for Standardization (ISO) and used in catalogues of international, regional, and national

standards and other normative documents. As part of this body of work, ICS heads up Information Technology. ISC 35.210, Cloud Computing, develops the following standards on Cloud SLAs.

- ISO/IEC JTC 1/SC 38 – Cloud Computing
- 19086-1, Cloud Computing – Service Level Agreement (SLA) Framework and Technology, Part 1: Overview and Concepts, Stage: Published September 2016
- 19086-2, Cloud Computing – Service Level Agreement (SLA) Framework and Technology, Part 2: Metrics, Stage: Published December 2018
- 19086-3, Cloud Computing – Service Level Agreement (SLA) Framework and Technology, Part 3: Core Conformance Requirements, Stage: Published July 2017
- 19086-4, Cloud Computing – Service Level Agreement (SLA) Framework and Technology, Part 4: Security and Privacy, Stage: Published January 2019

SLA Vocabulary

- Cloud Service Agreement (CSA) – Documented agreement between the cloud service provider and cloud service customer that governs the covered service(s)
- Cloud Service Level Agreement (SLA) – Part of the cloud service agreement that includes cloud service level objectives and cloud service qualitative objectives for the covered cloud service(s)
- Cloud Service Level Objectives (SLO) – Commitment a cloud service provider makes for a specific, quantitative characteristic of a cloud service, where the value follows the interval scale or ratio scale
- Cloud Service Qualitative Objectives (SQO) – Commitment a cloud service provider makes for a specific, qualitative characteristic of a cloud service where the value follows the nominal scale or ordinal scale

SLA Metrics

The definition and usage of appropriate metrics and their underlying measures and measurements are essential aspects of a cloud service SLA. The metrics are used to set the boundaries and margins of error and limitations. Examples of how metrics can be used include the following:

- Determine if SLOs are met
- Define a purpose for measures and measurements
- Deliver a consistent representation of measure and measurement information
- Link properties, measurements, and metrics
- Enable comparison of monitoring between services
- Determine cloud service effectiveness for business objectives

Construction of SLAs with 19086

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

Table 13: SLA Content Areas and Recommended SLOs and SQOs

SLA Content Areas	Cloud SLOs	Cloud SQOs
Accessibility	Accessibility Component	• Accessibility Standards • Accessibility Policies

Accessibility Attestations, Certifications, & Audits	Attestations, Certifications, & Audits	• Cloud Service Attestations • Cloud Service Certifications • Cloud Service Audits
Availability	Availability Component	• Availability
Cloud Service Support	Cloud Service Support	• Support Hours • Service Incident Support Hours • Service Incident Notification Time • Maximum First Support Response Time • Maximum Incident Resolution Time • Support Plans • Support Methods • Support Contacts • Service Incident Reporting • Service Incident Notification
Data Management	Intellectual Property Rights (IPR)	• Intellectual Property Rights
	Cloud Service Customer Data	• Cloud Service Customer Data • Cloud Service Customer Data Usage
	Cloud Service Provider Data	• Provider Data
	Account Data	• Account Data
	Derived Data	• Derived Data • Derived Data Usage • Derived Data Access
	Data Portability	• Data Portability Capabilities
	Data Deletion	• Data Deletion Time • Data Deletion Process • Data Deletion Notification
	Data Location	• Data Location • Data Location Specification Capability • Data Location Policy
	Data Examination	• Data Examination
	Law Enforcement Access	• Law Enforcement Requests
Governance	Governance Component	• Regulation Adherence • Standards Adherence • Policy Adherence • Audit Schedule
Performance and Verification	Cloud Service Response Time Component	• Cloud Service Maximum Response Time Observation • Cloud Service Response Time Mean • Cloud Service Response Time Variance
	Cloud Service Capacity Component	• Limit Simultaneous Cloud Service Connections • Limit Available Cloud Service Resources

		• Cloud Service Throughput • Cloud Service Bandwidth • Limit of Available Cloud Service Resources
	Elasticity Component	• Elasticity Speed • Elasticity Precision
Service Reliability and Verification	Service Resilience/Fault Tolerance	• Time to Service Recovery • Mean Time to Service Recovery • Maximum Time to Service Recovery • Number of Service Failures • Cloud Service Resilience/Fault Tolerance Methods
	Customer Data Backup and Restore	• Backup Interval • Retention Period for Backup Data • Number of Backup Generations • Backup Restoration Testing • Backup Method • Backup Verification • Backup Restoration Test Reporting • Alternative Methods for Data Recovery • Data Backup Storage Location
	Disaster Recovery	• Recovery Time Objective (RTO) • Recovery Point Objective (RPO) • Cloud Service Provider Disaster Recovery Plan
Termination of Service	Termination of Service Component	• Data Retention Period • Log Retention Period • Notification of Service Termination • Return of Assets
Change Management	Changes to the Cloud Service Features and Functionality	• Minimum Service Change Notification Period • Minimum Time Before Feature/Function Depreciation • Service Change Notification Method
PII Protection	PII Protection Component	• At the time of writing, PII SLOs and SQOs are under development by JTC1 SC27 and will be included in ISO/IEC 19086-4, "Information Technology – Cloud Computing – SLA Framework, Part 4: Security and Privacy" when published
Information Security	Information Security Component	• See Reference: DoD Cybersecurity T&E Guidebook, v2, April 2018; Addendum: Cybersecurity T&E of DoD Systems Hosted on Commercial Cloud Service Offerings

The following sections provide examples of select content areas.

Accessibility Content Area

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

Availability Content Area

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

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

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

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

NOTE: It is also referred to as "uptime percentage" and is often given over month-based billing period (i.e., monthly uptime percentage).

Important Information: This characteristic is common in current SLAs. It is an important characteristic. Although it can be complex, it can be measured without difficulty. There may be a time when the service is unavailable ("down") that does not count toward the total downtime (e.g., scheduled downtime). It is important to understand what counts as unavailable and how the unavailable periods are combined. Compute resources are often described using the time-based concept of availability while storage resources are often described using the transaction-based concept of availability. Example hours unavailable for common monthly uptime percentages (based on a thirty-day month) are below:

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

Cloud Service Performance Content Area

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

$$Tcsrt = 2Ttt + Trt$$

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

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

- Service Objectives.
  - Cloud Service Maximum Response Time Observation (SLO). The maximum time between a defined stimulus or input to the cloud service and a defined point in the response. The commitment the providers should give to provide a service where the measured service characteristic is lower than commitment value.

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

PMs should include cloud service maximum response time in the SLA. The commitment value should be based on the customer requirements and consider the effects of network transit time. PMs should use Metric T1 or T2.

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

<u>Capacity Component</u>

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

Protection of PII Content Area

- Protection of PII Component: The capability of the cloud computing service to protect personally identifiable information (PII). PII is defined in NIST SP 800-122 as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

Important Information: Protection of PII and PII management are important concepts and some language related to PII is likely included in a cloud contract in a clause or SOO/SOW/PWS.

- PII (SO)
  - At the time of writing, PII SLOs and SQOs are under development by JTC1 SC27 and will be included in ISO/IEC 19086-4, "Information Technology – Cloud Computing – SLA Framework, Part 4: Security and Privacy," when published.

Summary of Information and/or Actions Required for PMs

Table 14 summarizes specific information and/or requirements the PM needs to provide to the KO to enable the KO to execute a contract that protects DoD equities and minimizes risk.

Table 14: Information and/or Actions for PMs

Description	Information and/or Action
General Procedures for Cloud Services	• Determine IIL as detailed in the CC SRG. • Provide written justification as needed by KO.
Government Data & Government-Related Data	• Identify, document, and provide KO with unambiguous descriptions and formats of Government data and Government-related data needed to enforce all terms in clause where, "Government data and Government-related data" are referenced in DFARS 252.239-7010. • These descriptions and formats of Government data and Government-related data will be required by KO.
Security Requirements – Change in Representation DFARS 252.239-7010 (b) (1)	• Post contract award; if the contractor notifies the KO of a change in DFARS Provision 252.239-7009 then, it is likely that the entire approach will require reevaluation. • In collaboration with AO, reevaluate the proposed approach and determine if the change is acceptable. • Provide written notice and/or justification to support approval or disapproval decision to KO.
Security Requirements – Waiver DFARS 252.239-7010 (b) (2)	• Collaborate with AO and DoD CIO to determine and document what specific requirements of the CC SRG may/have been waived.

	• Provide KO with necessary documentation needed to specify extent and conditions of the DoD CIO waiver.
Location of Data – DFARS 252.239-7010 (b) (3)	• Collaborate with AO to determine (only for IIL-2 or IIL-4 data) if it is permitted to maintain Government data at a location outside the 50 States, the District of Columbia, and outlying areas of the United States. • Provide written justification as needed by KO.
Limitations on Access, Use and Disclosure DFARS 252.239-7010 (c) (1)	• Collaborate with AO to review and determine and unambiguously document if any access to or use of Government data or Government-related data requested or specified by contractor is permissible and if so, under what limitations and/or conditions. • Provide KO with documentation authorizing access.
Cyber Incident Reporting DFARS 252.239-7010 (d)	• Identify a Government point of contact (POC) for KO to contact if a cyber-incident occurs in connection with cloud services being provided. • If a cyber-incident occurs: – Procedures should be developed (to include mission owner, CSSP, and contractor) to collect, preserve, and protect Incident Information; these processes will vary depending on service model (IaaS, PaaS, and SaaS). – With the AO, CSSP, and the contractor, assess and determine the potential impact of the cyber incident and response.
Malicious Software DFARS 252.239-7010 (e)	• Collaborate with AO and other DoD entities to produce detailed instructions on submitting malicious software that was/may-have-been discovered in connection with a reportable cyber incident. • Provide the KO with the specific instructions produced.
Cyber Incident – Requesting Media and Data DFARS 252.239-7010 (f)	• Collaborate with AO and other DoD entities to determine if the media that was preserved and/or the data that was collected (when a cyber incident was discovered) is required by the DoD. • If required, instruct KO to request media and data from the contractor.
Cyber Incident – Access to Information or Equipment DFARS 252.239-7010 (g)	• Collaborate with AO and other DoD entities to determine if access to additional information or equipment is needed to conduct forensic analysis. • If needed, instruct KO to request access to additional information and/or equipment.
Cyber Incident – Damage Assessment DFARS 252.239-7010 (h)	• Collaborate with AO and other DoD entities to determine if damage assessment is required. • If damage assessment is required, inform KO to request damage assessment information from contractor. • Upon completion of damage assessment activities, provide the KO with a report documenting all findings that will be included in the contract files.
Records Management and Facility Access DFARS 252.239-7010 (i)	• When acquiring SaaS, provide a records retention schedule to the KO to be incorporated in the contract that includes, but is not limited to, secure storage, ability to retrieve, and proper disposition of all federal records. KOs should coordinate with customer records management staff to provide a National Archives-approved Records Control Schedule(s) (RCS) for the records covered in the acquisition. • When acquiring IaaS/PaaS, maintain a copy of the contractor's and/or cloud service provider's data retention policies for Government-related data. If the contractor's and/or cloud service provider's data retention policies are shorter than the National Archives-approved records retention time for the Government-related data, coordinate with the contractor and/or cloud service provider on a process to store the Government-related data to an alternate storage location.

Records Management – Format of Data DFARS 252.239-7010 (i) (1)	• Collaborate with AO and all other related DoD stakeholders to provide the KO with unambiguous description of formats of Government data and Government-related data needed to enforce the terms in clause.
Records Management – Contract Closeout DFARS 252.239-7010 (i) (2)	• Collaborate with AO and, if necessary, the Component Records Management Officer (CMRO), to determine how Government data and Government-related data is to be handled during contract closeout. • Provide KO with unambiguous description of how contractor is to transfer, retain, or dispose and confirm disposal of Government data and Government-related data as part of contract closeout needed to enforce the terms in clause.
Records Management – Required Accesses to … DFARS 252.239-7010 (i) (3)	• Collaborate with AO and all other DoD entities to identify and ensure that all Government or its authorized representatives have determined and documented what physical, system, and/or system-wide accesses and response timeframes the contractor will need to provide in order to support their lawful activities. • Provide KO with unambiguous description of all accesses and timeframes required in the contract/SLA.
Notification Of Third Party Access Requests DFARS 252.239-7010 (j)	• Identify the Government POC responsible for coordinating the response to any subpoena or other third party access received by the contractor providing the cloud service. • Provide KO with the Government POC. • **If third party access request is received:** – Coordinate the response with the DoD mission or data owner.
Spillage DFARS 252.239-7010 (k)	• Identify the contractor POC and Government POC to contact if any spillage occurs regarding the cloud service being provided. • Provide KO with the POCs and procedures needed to enforce the terms in clause. • Ensure that agency procedures for addressing a spillage are documented. • **If spillage occurs:** – Follow agency procedures.
Subcontracts DFARS 252.239-7010 (l)	• Provide KO with requirements related to flow down when contracting for PaaS or SaaS which leverages an IaaS or PaaS from a third party cloud service provider.
Contractor Terms and Conditions - Terms Of Service Subpart 239.7601-1 (a)	• Collaborate with AO to review contractor's Terms of Service and produce document detailing where they may be found to impede or conflict with mission and cyber security requirements. • Provide KO with the document to ensure conflicts are resolved as part of the other processes the KO needs to perform in order to meet the intent of this Subpart.
Inspection, Audit, Investigation Support Subpart 239.7601-1 (c) (3)	• Provide KO with requirements to support authorized activities regarding Government data or Government-related data, or cloud service offering service model.
Inspection, Audit, Investigation Search & Access Subpart 239.7601-1 (c) (4)	• Provide KO with requirements to support and cooperate with authorized activities' system-wide search and access.
Other Consideration – Cybersecurity Compliance CC – SRG	• Collaborate with AO to ensure that cybersecurity requirements or processes not otherwise addressed in the CC SRG and DoD provisional authorization assessment are documented. PMs must ensure that issues identified throughout the life of the contract that may adversely impact the cloud service offering/mission risk, and thereby, jeopardize the validity of the ATO,

	are addressed in the contract/SLA. For example, if DISA discovers that the cloud service provider is not meeting ongoing security requirements, they will notify affected Mission Owners/PMs and work with the cloud service provider to develop a corrective Plan of Action and Milestones (POA&M). – Review DISA's assessment of the contractor's corrective POA&M. – Collaborate with AO to make a risk determination with regard to their specific usage of the cloud service offering and ATO. – Collaborate with AO and KO to determine if contracting action to incorporate the cloud service provider's POA&M is needed; annotate contract files as needed.
Change In CSP Ownership CC – SRG	• Collaborate with AO to determine how to address the impact of a change of ownership of the cloud service provider. If such change necessitates off-boarding and retrieval of information/data, produce document that describes how the contractor is to transfer, retain, or dispose and confirm disposal of Government data and Government-related data. • Provide KO with the document so that off-boarding processes can be reflected in the contract/SLA.
Disaster recovery (DR) and Continuity of Operations (COOP)	• As a best business practice, require that the contractor (cloud service provider or third party) plans for Disaster Recovery (DR) and Continuity of Operations (COOP) and implements their infrastructures to support it.
Exit Process	• Provide KO with unambiguous document describing how contractor is to transfer, retain, or dispose and confirm disposal of Government data and Government-related data and/or migrate applications upon completion or termination of the contract. • Provide KO with the document so that closeout processes can be reflected in the contract/SLA.

7. Additional Resources

The Requirements for the Acquisition of Digital Capabilities Guidebook is an iterative document updated on an ad-hoc basis as policies, guidance, and the digital world continue to evolve.

The Defense Acquisition University, DoD Cloud Computing Acquisition Guidebook, provided the content for Section 6, Cloud Acquisition Guidance, and is available for reference with additional details and examples.

Table 15: Resources

Linked Resource	Description
DoD Digital Modernization	Online location of strategy and sub-strategies
DoD Software Modernization	Online location of DoD Software Modernization Strategy
Clinger Cohen Act Compliance	Documentation for Clinger Cohen Act compliance for each pathway
DITIP/SNaP-IT	IT Investment Reporting Tool for PPBE (only available on NIPR)
DITPR/SITPR	DoD IT Portfolio Repository
Information Enterprise Architecture (IEA)	Online location of the IEA and associated architecture guidance (e.g., reference architectures and reference designs) (CAC required)
DoD IT Standards Registry	Registry of DoD-approved IT standards (CAC required)
Enterprise Software Initiative	Online location for enterprise licensing agreements
Risk Management Framework (RMF) Knowledge Service	Online location for risk management framework guidance
Supply Chain Risk Management Portal	Online location for supply chain risk management (CAC required)
https://www.data.mil	Online location for additional data guidance
ADVANA	Location of federated data catalog and other analytics capabilities

DCIM	Data Center Inventory management System
IT Purchase Request Tool	Online application for requesting approval of IT purchase requests
Linked Cloud Resources	**Description**
NIST SP 8000-145	The NIST Definition of Cloud Computing
NIST SP 500-292	NIST Cloud Computing Reference Architecture
DFARS Subpart 239.76	Cloud Computing
DFARS 252.239-7009	Representation of Use of Cloud Computing
DFARS 252.239-7010	Cloud Computing Services
DFARS PGI 239.76	Cloud Computing
CC SRG	DoD Cloud Computing Security Requirements Guide
https://www.cloud.mil	List of available enterprise cloud contracts
DoDCIO.Cloud.Team@mail.mil	Email for questions concerning DoD cloud policy
System Network Approval Process (SNAP)	System for Registering Cloud Service Offering prior to connecting a cloud service to a DoD network (only available on NIPR)
FedRAMP Marketplace	List of FedRAMP-approved cloud services
DISA Cloud Service Offering Catalog	List of DISA provisionally authorized cloud service offerings
Cybersecurity Service Provider (CSSP)	List of available CSSPs

8. Version and Revision History

Version #	Revision Date	Reason
0	11/12/2016	• Chapter 6 initial upload
0	02/01/2017	• CH 6–3.9.2 Cloud Computing–links validation
0	09/29/2017	• Chapter links validated/updated and “shortcut” where appropriate.
1.0	11/27/2017	• Updates to DoDI 5000.75/Business Capability Acquisition Cycle (BCAC) • Updates to cloud, enterprise services, and interoperability content
1.1	01/25/2018	• Updates to MAIS language per repeal of Chapter 144A in the FY2017 NDAA. • Updates to MAIS/DBS language per removal of MAIS/DBS from MDAP definition in FY2018 NDAA. • Link updates and other standard formatting updates
1.2	09/30/2019	• Adds Chapter 6-3.9.3, Acquisition of Internet Protocol Version 6 (IPv6) Capable Products • Adds Chapter 6-4.6 Acquisition Policy Evolution to an Adaptive Acquisition Framework • Updates Figure 6, BCAC for DBS • Minor edits for currency
1.0	1/3/2022	• Rewrites and modernizes Chapter 6 in alignment with Adaptive Acquisition Framework • Renames document to Requirements for the Acquisition of Digital Capabilities Guidebook • Updates reflect DoDI 5000.82