DISA
DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Acquiring Cloud Services

A Contracting Officer's perspective

Scott M. Stewart
Technical Director
Procurement Services Directorate

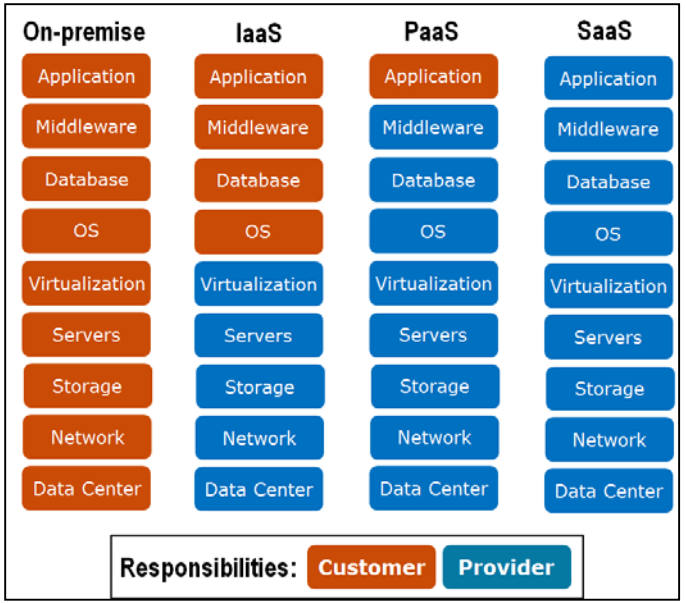
16 May 2018

Agenda

- Service and Deployment Models and why they matter
- Security, Data Characterizations, and Impact Levels
- Acquisition Guidance and Regulations
- Process for Acquiring Cloud Services
- Summary
- Questions

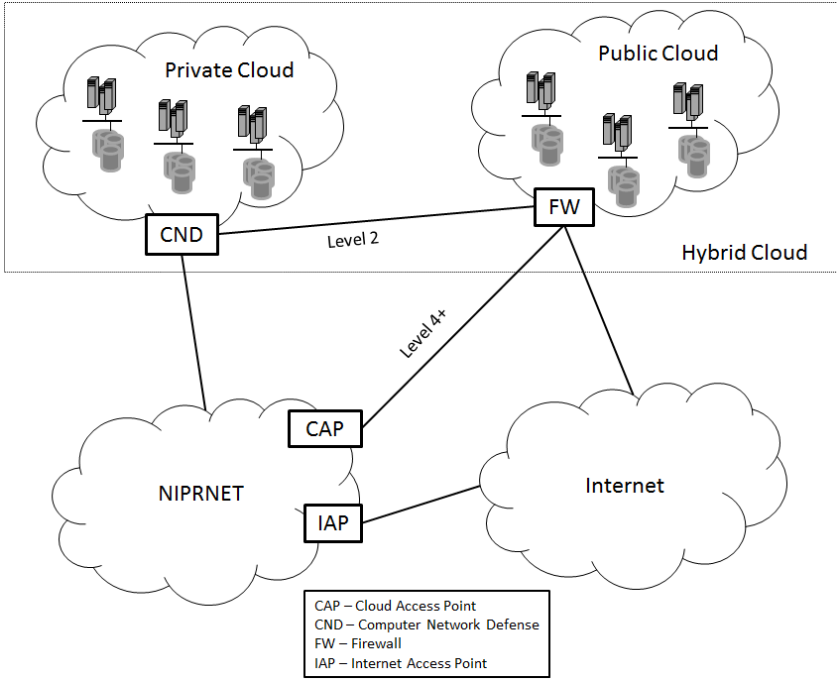
There are three primary cloud service models: IaaS, PaaS, and SaaS

- **Infrastructure as a Service**
  - Virtual Servers
  - Storage Services
  - Network Services
- **Platform as a Service**
  - Application Development Servers
  - Programming Support
  - Developer Services
  - Data Services
- **Software as a Service**
  - Office Automation
  - Enterprise Mission Applications
  - Communications Services



There are also several options for deploying cloud services

- **Private Cloud – Infrastructure is deployed solely for a single customer's requirements**
- **Public Cloud – Infrastructure is shared by diverse tenants at cloud service provider's facilities**
- **Community Cloud – Infrastructure is shared by similar types of tenants with similar requirements (e.g. the DoD Milcloud)**
- **Hybrid Cloud – Customer's IT infrastructure includes both Private Cloud and Public Cloud, more sensitive processing and data are kept on Private Cloud, less sensitive processing is performed on Public Cloud (Public Cloud can be used to handle non-sensitive surge)**



The Contracting Officer (KO) should be familiar with several cloud services security initiatives

- **FedRAMP - A government-wide program that provides a standardized approach to security for cloud services. DOD leverages FedRAMP and other Federal Agency security documentation residing in the FedRAMP Secure Repository when it conducts security assessments. DoD adds security controls to FedRAMP to meet its additional security requirements, known as FedRAMP+**
- **DoD Provisional Authorization – Provided to non-DoD cloud service offerings that have properly implemented the FedRAMP controls and the additional controls and requirements of the *DoD Cloud Computing Security Requirements Guide***
- **Cloud Access Point – For Level 4 and above cloud service offerings (CSOs), provides a barrier of protection between the DOD and DOD use of commercial cloud services. The CAP will proactively and reactively prevent attacks against the DODIN infrastructure and mission applications**

The security Impact Level of the system to be deployed will affect procurement

IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	DEPLOYMENT MODELS	PERSONNEL REQUIREMENTS
1	----------Impact Level Deprecated----------					
2	PUBLIC or Non-critical Mission Information	FedRAMP v2 Moderate	US / US outlying areas or DoD on-premises	Internet	PUBLIC	National Agency Check and Inquiries (NACI)
3	----------Impact Level Deprecated----------					
4	CUI or Non-CUI Critical Mission Information Non-National Security Systems	Level 2 + CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	COMMUNITY or PRIVATE DoD and Federal Government Tenants Only	ADP-1 Single Scope Background Investigation (SSBI) ADP-2 National Agency Check with Law and Credit (NACLC) Non-Disclosure Agreement (NDA)
5	Higher Sensitivity CUI National Security Systems	Level 4 + NSS & CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	COMMUNITY or PRIVATE DoD and Federal Government Tenants Only	
6	Classified SECRET National Security Systems	Level 5 + Classified Overlay	US / US outlying areas or DoD on-premises CLEARED / CLASSIFIED FACILITIES	SIPRNET via CAP	COMMUNITY or PRIVATE DoD and Federal Government Tenants Only	Favorably Adjudicated SSBI SECRET Clearance NDA

Examples of Different Systems

Level 3 Examples

- Executive Dining Facilities
- Marine Corps Marathon Automated Support System
- DON Family Support Program Volunteers

Level 4 Examples

- Army Training Requirements and Resources System
- Lodging Reservations System
- Voluntary Leave Transfer Program

Level 5 Examples

- Defense Clearance and Investigations Index (DCII)
- Defense Civilian Pay System (DCPS)
- Air-to-Air Weapon System Evaluation Program Records

For more information refer to DoD Manual 5200.01, Volume 4, Feb 24, 2012

The KO should be familiar with relevant acquisition regulations and guidance

- **DOD organizations are responsible for acquiring the cloud services that meet their mission objectives and provide an optimal solution compliant with DOD and other federal regulations**
- **Important cloud related guidance documents**
  - **Defense Acquisition Guidebook (DAG) Chapter 6-3.9.2, Cloud Computing**
  - **DoD Cloud Computing Security Requirements Guide**
  - **DoD Instruction 5000.74, “Defense Acquisition of Services”, October 5, 2017, Enclosure 7 identified IT considerations in the acquisition of IT services that includes cloud services.**
  - **Defense FAR Supplemental (DFARS) 239.76 Cloud Computing and DPAP PGI 239.76**
  - **FedRAMP Control Specific Contract Clauses, Version 3, December 8, 2017**
  - **DISA Cloud Connection Process Guide (CCPG), Version 2, March 2017**

Key areas that the KO needs to address in the procurement of Cloud Services

- Availability and Availability Reporting of the Cloud Services
- A Business Case Analysis needs to be developed
- Protection of Government Data
- Include Indemnification Clauses in Contract
- Access to Government Data for Law Enforcement and Other Purposes
- Location of Government Data
- Government Records Management Policies
- Support of Government Security Regulations
- Defining Service Level Agreements (SLA)
- Government Documentation of DoD Cloud Services Procured
- Subcontracting Rules
- Supply Chain Management
- Terms of Service

The KO must define the availability and availability reporting requirements

- **Service Interruption Reporting – The Contractor must inform the Government of any interruption in the availability of the cloud service as required by the service level agreement.**
- **Outage Estimate – Whenever there is an interruption in service, the Contractor shall inform the Government of the estimated time that the system or data will be unavailable.**
- **System Availability Requirements – The estimated timeframe for recovery of the service must be related to the FIPS 199 system categorization for the availability of the system, and if specified, the Contractor shall meet the agreed upon service level and system availability requirements.**
- **System Availability Updates - 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.**

The organization shall prepare a Business Case Analysis (BCA) for Cloud Services

- **A BCA is required by *DoD CIO Memo, Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services*, December 15, 2014**
- **It provides an analysis of the cloud services requested using the DoD CIO IT Business Case Analysis (BCA) template**
- **Consider DISA provided cloud services as an alternative in the BCA**
- **Have the approval of the Component CIO**
- **Provide a copy of the BCA to the DoD CIO**

The KO must ensure protection for government data

- **Protection of government data is required by the *Federal Acquisition Regulations (FAR) Procedures, Guidance, and Information (PGI)***
- **Data ownership, licensing, delivery and disposition instructions specific to the relevant types of Government data and Government-related data shall be part of the contract**
- **Appropriate limitations and requirements regarding contractor and third-party access to, and use and disclosure of, Government data and Government-related data shall be documented in the contract**
- **Appropriate requirements to support applicable inspection, audit, investigation, or other similar authorized activities specific to the relevant types of Government data and Government-related data, or specific to the type of cloud computing services being acquired**
- **Appropriate requirements to support and cooperate with applicable system-wide search and access capabilities for inspections, audits, investigations, litigation, eDiscovery, FOIA requests, records management associated with the agency's retention schedules, and similar authorized activities**
- **A requirement for the contractor to coordinate with the responsible Government official designated by the contracting officer, in accordance with agency procedures, to respond to any spillage occurring in connection with the cloud computing services being provided**
- **A requirement that the Contractor shall use Government-related data only to manage the operational environment that supports the Government data and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer.**

Include indemnification clauses in the contract to protect the government (sample text)

- **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**
- **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 Contract Officer, all evidence and information in the Contractor's possession pertaining to such claim or suit.**
- **Further, this indemnity shall not apply to a disclosure or inclusion of data or information upon specific written instructions of the Contract Officer directing the disclosure or inclusion of such information or data; 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.**

The KO shall ensure the CSP provides immediate access to government data (sample text)

- **As specified by the Contract Officer, the Contractor shall provide immediate access to all Government data and Government-related data affecting 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 Contract Officer, and without the Contractor's involvement.**
- **The Contractor shall record all physical access to the cloud storage facilities and all logical access to the government data as specified in the contract.**

The KO must ensure the Government knows where government data is stored and processed

- **In accordance with the Defense Federal Acquisition Regulation Supplement (DFARS), the Contract Officer must ensure that the contract with the CSP specifies that the Contractor shall maintain within the United States or outlying areas all Government data that is not physically located on DOD premises, unless the Contractor receives written notification from the Contracting Officer to use another location.**
- **More sensitive government data may have further restrictions on the location of data, work with security to define location requirements**

The CSO shall support government record management policies (sample text)

To comply with a variety of rules and regulations federal managers must ensure contractors properly manage, secure, and process federal records IAW the provisions of DoDI 5015.02

- **The Contractor shall provide the Contracting Officer all Government data and Government-related data in the format specified in the contract or as directed by the Contract Officer.**
- **The Contractor shall dispose of Government data and Government-related data in accordance with the contract and provide the confirmation of disposition to the Contract Officer in accordance with contract closeout procedures.**
- **The Contract 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 the Contractor is notified in writing by the Contract Officer, and shall preserve all such data in accordance with agency instructions.**
- **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.**

The Contract with the CSO shall support government security requirements

- To comply with a variety of rules and regulations it is important that federal managers ensure contractors properly manage, secure, and process federal records IAW the provisions of DoDI 5015.02
- The Contractor shall provide the Contract Officer all Government data and Government-related data in the format specified in the contract or as directed by the Contract Officer.
- The Contractor shall dispose of Government data and Government-related data in accordance with the contract and provide the confirmation of disposition to the Contract Officer in accordance with contract closeout procedures.
- The Contract 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 the Contractor is notified in writing by the Contract Officer, and shall preserve all such data in accordance with agency instructions.
- 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.

Summary of Guidance and Regulations

Security	Privacy	Law Enforcement	Admin
*Non-Disclosure**	Org Conflict of Interest*	Physical Access	*Operational Control (Use of Subcontractors)**
Spillage	Data Breach*	Law Enforcement Access*	Record Management*
*Supply Chain Risk Management**	*Insurance**	*Facility Inspections*	*Terms of Service*
*Maintenance**		*Location of Data*	*Indemnification**
*FISMA Compliance**		Notification	
*Continuous Monitoring**		*Banner**	
*Asset Availability**			
Personnel Access			

The guidance marked in green were incorporated into DFARS 239.6 The orange blocks remain guidance and should be incorporated into the contract PWS. Asterisk indicates a portion of the original guidance were made regulatory while the remaining language is guidance.

The Component must properly document the cloud service offering

- **SNAP - The CSO needs to be documented in the Systems Network Approval Process (SNAP) database, so that DISA, on behalf of the DoD CIO can track all CSPs hosting DOD information and for the DoD Information Network (DoDIN) documentation and tracking purposes. SNAP is an OSD/CAPE web tool on both SIPRNET & NIPRNET**
- **SNaP-IT (Select and Native Programming Data Input System for Information Technology) - The Component must report the procurement of cloud services. The SNaP-IT repository is a DOD CIO tool and is the authoritative source of budget information about DOD IT that is used for reporting to Congress and OMB.**
- **FedRAMP - The Component's Security Team should document the security assessment documentation in the FedRAMP Secure Repository for the benefit of other US Federal organizations**

The CO shall ensure the CSP includes government contract requirements in all subcontracts (sample text)

The Contract Officer must ensure that the Contractor includes government contract requirements in all subcontracts, including subcontracts for commercial items.

- **The Contractor shall retain operational configuration and control of data repository systems used to process and store government data to include any remote work.**
- **The Contractor shall not subcontract the operational configuration and control of any government data.**

Disadvantages of using Intermediaries: No privity of contact

Actual service provider not liable to the Government for the terms and condition within the Government Contract

- **Not directly accountable to the Government for:**
  - **Service Level Agreements**
  - **Pricing clauses and notice of pricing changes**
  - **Insurance and indemnification clauses**
  - **Data assurance requirements (e.g., data ownership, data location requirements, disposition requirements, spillage response)**
  - **Functionality and notice of substantive change**
  - **Security monitoring requirements**
  - **Employee requirements (e.g., US Persons) and privileged access requirements**
  - **Disaster recovery requirements**
  - **Inspection, forensics and audit requirements**
  - **Modification of term and conditions**
  - **Notification of pending mergers and acquisitions**
- **Government's only recourse is with the Intermediary**

  From actual Cloud Access Policy: "We have no obligation to provide service to you, so you must look exclusively to your reseller and your agreement with your reseller regarding such obligation."

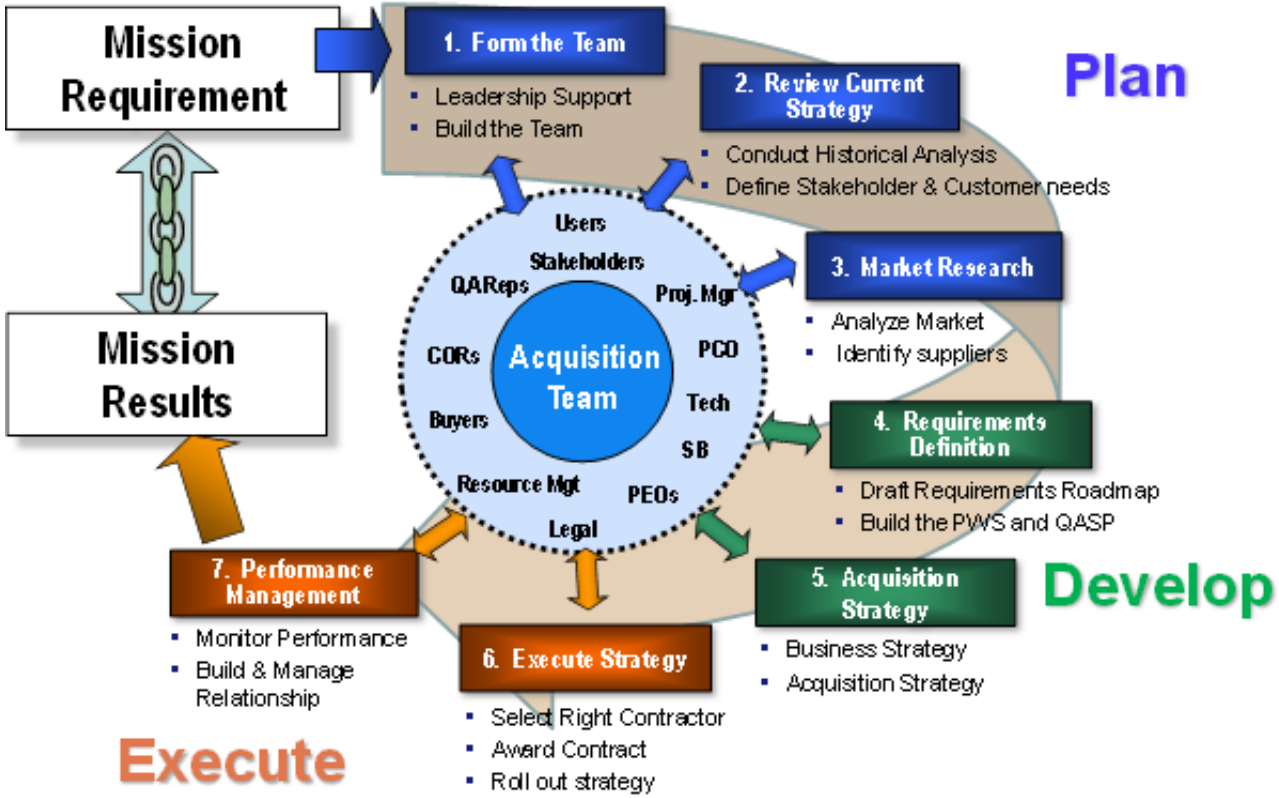
The KO must ensure that the CSP can manage its supply chain appropriately (sample text)

- **The Contractor shall submit a Supply Chain Risk Management (SCRM) plan as part of its technical proposal.**
- **The plan shall include the criticality analysis (CA) process used by the offeror to determine Mission Critical Functions and the protection techniques**
- **The 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**
- **The 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.**
- **The plan shall identify the relationship between the offeror and the manufacturer**
- **The Contractor SCRM plan shall include the offeror's expressed warranty that the software shall be free from all computer harmful or malicious code**
- **The Contractor shall incorporate the substance of the Supply Chain clauses in subcontracts**
- **All subcontractors providing critical components or services shall be identified**

The KO must ensure TOs are compliant with federal regulations

- **Although DOD may generally accept commercial terms & conditions, many commercial services have Terms of Service Agreements that contain clauses that the government cannot accept – either because they are inconsistent with federal law or regulation, or do not meet the Agency's needs**
- **Contracting officers must incorporate any applicable service provider terms and conditions into the contract by attachment or other appropriate mechanism**
- **Contracting officers must carefully review commercial terms and conditions and consult legal counsel to ensure these are consistent with Federal law, regulation, and the agency's needs**
- **At the termination of the contract, the service provider shall return the Agency's data in a format and in a manner previously agreed upon with no additional fees**
- **The Contracting Officer must ensure that the contract clearly identifies who owns any customizations or enhancements**

The acquisition of cloud services should follow the standard DoD process for acquiring IT Services



Key Cloud Service Acquisition Activities

	Form the Team	Review Current Strategy	Market Research	Requirements Definition	Acquisition Strategy	Execute Strategy	Manage Performance
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**

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

www.disa.mil **/USDISA** **@USDISA**