
Vicki Allums
Learning Director, Intellectual Property
July 24, 2019
Commercial Cloud Computing Acquisitions

- DoD Policy
  - “Accelerating Enterprise Cloud Adoption,” September 13, 2017
  - “DoD Cloud Update,” June 22, 2018

- Key Questions -- Cloud Computing Acquisitions
  1) What is cloud computing?
  2) What are the primary service models?
  3) How do security considerations impact acquisitions?
  4) What are the critical contract considerations in commercial cloud acquisitions?
  5) What are the intellectual property/data rights issues?

**Goal: -- Best practices & Lessons Learned**
Acquiring Cloud Solutions

A Contracting Officer’s and Attorney’s perspective

Scott M. Stewart, DISA PSD Tech Director
Jodi Cramer, Senior Air Staff Counsel
Carrie Ross, DISA Contracting Officer
July 24, 2019
Three Primary Service Models

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

Responsibilities: Customer Provider
Consumption-based Solutions

- Problem: The FAR unrealistically categorizes all purchases as either *supplies* or *services*, a decades-old distinction that is too rigid to effectively procure modern technology solutions with evolving delivery models.

- What you can do now:
  - Use a FAR deviation to permit a new contract type called *fixed-price resource units* that:
    - Establishes a fixed price per unit of measure and captures commercial price reductions
    - Sets a ceiling for the overall contract value against which consumption of individual resource line items will be charged
    - Can be incrementally funded
    - Is paid in arrears based on actual consumption
  - Actively manage consumption using available vendor tools (e.g., set limits by user or group, contractor notify the government when consumption reaches 75 percent and 90 percent of the contract funded amount)
## System Security Impact Level

<table>
<thead>
<tr>
<th>IMPACT LEVEL</th>
<th>INFORMATION SENSITIVITY</th>
<th>SECURITY CONTROLS</th>
<th>LOCATION</th>
<th>OFF-PREMISES CONNECTIVITY</th>
<th>DEPLOYMENT MODELS</th>
<th>PERSONNEL REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Public or Non-critical Mission Information</td>
<td>FedRAMP v2 Moderate</td>
<td>US / US outlying areas or DoD on-premises</td>
<td>Internet</td>
<td>PUBLIC</td>
<td>National Agency Check and Inquiries (NACI)</td>
</tr>
<tr>
<td>2</td>
<td>CUI or Non-CUI Critical Mission Information</td>
<td>Level 2</td>
<td>US / US outlying areas or DoD on-premises</td>
<td>NIPRNet via CAP</td>
<td></td>
<td>ADP-1 Single Scope Background Investigation (SSBI)</td>
</tr>
<tr>
<td></td>
<td>Non-National Security Systems</td>
<td>CUI-Specific Tailored Set</td>
<td></td>
<td></td>
<td></td>
<td>ADP-2 National Agency Check with Law and Credit (NACLC)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US / US outlying areas or DoD on-premises</td>
<td></td>
<td></td>
<td></td>
<td>Non-Disclosure Agreement (NDA)</td>
</tr>
<tr>
<td>4</td>
<td>Higher Sensitivity CUI National Security Systems</td>
<td>Level 2</td>
<td>US / US outlying areas or DoD on-premises</td>
<td>NIPRNet via CAP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CUI-Specific Tailored Set</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Classified SECRET National Security Systems</td>
<td>Level 5</td>
<td>US / US outlying areas or DoD on-premises</td>
<td>SIPRNET via CAP</td>
<td></td>
<td>Favorably Adjudicated SSBI SECRET Clearance NDA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Classified Overlay</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Commercial Cloud Considerations

- DFARS CLAUSE – 239.76
  - Physical Access
  - OCI
  - Data Breach
  - Facility Inspection
  - Law Enforcement
  - Notification
  - Records Management
  - Spillage

- DoD Cloud SRG
  - Personnel Access
  - Jurisdiction
  - SCRM
Commercial Cloud Considerations (Cont’d)

- Additional DoD Identified
  - NDA
  - Asset Availability
  - Banner
  - Continuous Monitoring
  - Compliance
  - Direct Relationship
  - Indemnification
  - Cyber Insurance
  - Maintenance
  - TOS

- GAO
  - Stakeholder Roles And Responsibilities
  - Terms And Dates
  - Measurable Performance Objectives
  - Access To Agency Data
  - Service Management Requirements
  - Disaster Recovery Planning
  - Exception Criteria
  - Security Performance Requirements
  - Notification of Security Breach
  - Consequences
12 Possible SLA Content Areas

- Accessibility
- Availability
- Performance
- Service Reliability
- Data Management
- Attestations, Certs, & Audits
- Change Management
- Cloud Service Support
- Governance
- Termination of Service
- PII Protection
- Information Security
- Security
Examination of SLA Content Areas

- **Accessibility**
  - Accessibility Component
  - Accessibility Standards
  - Accessibility Policies
- **Availability**
  - Availability Component
  - Availability
  - Cloud Service Response Time Component
    - Cloud Service Response Time Observation
    - Cloud Service Response Time Mean
    - Cloud Service Response Time Variance
- **Performance**
  - Performance
  - Cloud Service Capacity Component
    - Limit of Simultaneous Cloud Service Connections
    - Limit of Available Cloud Service Resources
    - Cloud Service Throughput
    - Cloud Service Bandwidth
- **Elasticity**
  - Elasticity Component
    - Elasticity Speed
    - Elasticity Precision
- **Service Reliability**
  - Service Reliability
  - Service resilience/fault tolerance
    - Time to Service Recovery
    - Mean Time to Service Recovery
    - Maximum Time to Service Recovery
    - Number of Service Failures
    - Cloud Service Resiliency/Fault Tolerance methods
      - Backup Interval
      - Retention Period for Backup Data
      - Number of Backup Generations
      - Backup Restoration Testing
      - Backup Method
      - Backup Verification
      - Backup Restoration Test Reporting
      - Alternative Methods for data recovery
      - Data Backup Storage Location
  - Customer data backup and restore
    - Backup Time Objective (RTO)
    - Recovery Point Objective (RPO)
    - Cloud Service Provider Disaster Recovery Plan
- **Data Management**
  - Data Management
- **Governance**
  - Cloud Service Support
- **Changes to the cloud service features and functionality**
  - Attestations, Certifications and Audits
  - Termination of Service
  - PII Protection
  - Information Security
Contract Innovations

• **Problem:** How does the Government capture the innovations of the commercial cloud into a successful Government contract?

• **Building Blocks to Cloud:**
  – Innovation involves a team
  – Let the Contract work for you
    • Blanket Purchase Agreement or Indefinite Delivery Indefinite Quantity
    • Commercial parity with industry best practices
    • Protecting the Governments Rights
      – Cloud Insurance
      – FAR/DFAR Clauses
    • Identify all your needs up front
Contracting Innovations

- Paying for Cloud
  - Monitor applications and services
    - Pay as you go
    - Self-Management tools
  - Defined CLINs/SLINs
    - 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
Acquisition Planning

milCloud ® 2.0

Vera Strebel
Deputy Legal Counsel
July 24, 2019
PLANNING PHASE

- **Know your requirements**
  - Acceptable vs. Unacceptable

- **Primary User / Users**
  - User Requirements
  - Flexibility: payment and usage

- **Type of Contract**
  - IDIQ (single award vs. multiple award)
    - Harris IT Protest
  - Solution-based vs. Specific Requirements
    - Contractor Owned, Contractor Operated solution

- **Type of Contractor**
  - Qualifying Criteria

- **Time**
  - Planning/Evaluations/Litigation
Contracting Innovations

• Teams
  ▪ Technical
  ▪ Past Performance
  ▪ Cost/Price
  ▪ Contracting

• Leadership
  – Expectations

• Communications
  – Common Goals / Objectives
  – Thinking like an engineer/computer scientist

• Documentation

Communication is KEY

Evaluation Criteria

- Qualifying Criteria
  - Factor 1: Technical
    - Subfactor 1: DoD Level 5 PA
    - Subfactor 2: Initial Operating Capability (IOC)
    - Subfactor 3: Business Management
    - Subfactor 4: Transition Support
  - Factor 2: Past Performance
  - Factor 3: Small Business Management
  - Factor 4: Cost/Price
DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

www.disa.mil /USDISA @USDISA
Intellectual Property and Data Rights Considerations in Cloud Computing Contracts

Vicki Allums
Learning Director, Intellectual Property
July 24, 2019
“IP Strategy” -- Acquisition Consideration & Planning

• “IP Strategy” a critical component of Acquisition Strategy

• Critical Questions
  1) What type of service model (e.g. IaaS, PaaS, SaaS)
  2) What are the technology components (e.g. hardware, software technical data)
  Are the technology components GOTS, COTS or a hybrid?
  4) Do the technology components need to be reconfigured (or integrated) for the Government environment?
  5) What is the scope of the reconfigurations and integration?
  6) What are the IP licensing terms and obligations?
Protecting the Government’s IP/Data Rights Interests

• Contract Provision -- Section H
  • Detailed list of all technology components
  • Contractor obligation - technology components ("License agreement")
  • Use of third-party vendor technology -- component list and license agreements
  • Identify integration, reconfiguration & segregability of technology components
  • DFARs clauses (e.g. 252.227-7013, 252.227-7014, 252.227-7015)
Other IP Considerations

• Data content and usage issues
• Protecting IP in the cloud – security protocols and data access
• Contractor Managed Program
  • Program name Usage Issues
• Review SLAs for IP terms and obligations

Having an IP Strategy is the Key!