## Policy and PWS Language

<table>
<thead>
<tr>
<th>Subject Area</th>
<th>Policy</th>
<th>Policy Reference/Source (AR, DFARS, AFARS, DOD, etc.)</th>
<th>PWS language</th>
<th>Building Blocks</th>
<th>Contract Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cloud</strong></td>
<td>All commercial cloud usage must be reported into the Army Portfolio Management System (APMS) per data EXORD 009-20</td>
<td>EXORD 009-20</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Use of Enterprise Services</strong></td>
<td>All Army systems/applications developed, migrated to and hosted in the commercial cloud will use Army Enterprise common services and data services. The Army will not duplicate common services or data services that are accredited in Army.</td>
<td>EXORD 009-20; 3 D.5.G. (C) DIRECT THE ENTERPRISE CLOUD MANAGEMENT OFFICE (ECCMO) TO DEVELOP A PLAN TO CONSOLIDATE EXISTING CLOUD INSTANCES TO THE GREATEST POSSIBLE EXTENT, AND WITHOUT SIGNIFICANT IMPACT TO CONTINUING OPERATIONS, TO GAIN VISIBILITY AND CONTROL OF ARMY CLOUD MIGRATIONS NLT 01 JAN 2020.</td>
<td>The contractor must use Army Enterprise common services, and data services, and all DoD Secure Cloud Computing Architecture (SCCA) components when developing, migrating to and hosting Army systems/applications in the commercial cloud. A list of the currently available common services is included in the next tab in this spreadsheet. In the future, a dynamic website will be available that will include up-to-date listing and description of available Enterprise services: <a href="http://www.cloud.army.mil">www.cloud.army.mil</a>.</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td><strong>Use of Enterprise Services</strong></td>
<td>Existing cloud common services will be consolidated into Army as is reasonable over time, per EXORD 009-20. As existing common service contract options expire, mission owners should work with the Enterprise Cloud Management Office (ECMO) to coordinate their applications into Army, and reduce the duality of services across the Army.</td>
<td>EXORD 009-20; 3 D.5.G. (C) DIRECT THE ENTERPRISE CLOUD MANAGEMENT OFFICE (ECCMO) TO DEVELOP A PLAN TO CONSOLIDATE EXISTING CLOUD INSTANCES TO THE GREATEST POSSIBLE EXTENT, AND WITHOUT SIGNIFICANT IMPACT TO CONTINUING OPERATIONS, TO GAIN VISIBILITY AND CONTROL OF ARMY CLOUD MIGRATIONS NLT 01 JAN 2020.</td>
<td>N/A</td>
<td>N/A</td>
<td>Required</td>
</tr>
<tr>
<td>Modernization/Migration</td>
<td>The Army will modernize applications applying Cloud Native Design Principles, which will prioritize the use of Software as a Service (SaaS) and Platform as a Service (PaaS) to include container technology over Infrastructure as a Service (IaaS) models to reduce tool and overhead of maintaining Information Technology (IT) systems. Use of cloud will be by exception and at the approval of the Army Cloud Plan. By exception, applications that are too small to be economical or technically feasible.</td>
<td>Army Cloud Plan</td>
<td>The contractor must modernize applications applying Cloud Native Design Principles and will prioritize use of Software as a Service (SaaS) and Platform as a Service (PaaS) over Infrastructure as a Service (IaaS).</td>
<td>Mandatory</td>
<td>N/A</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Modernization/Migration</td>
<td>Legacy systems undergoing modifications to adapt to a service-oriented architecture should design with anti-corruption layers to support the transitional period. Pre-built COTS products are excluded.</td>
<td>Army Cloud Plan</td>
<td>The contractor must ensure that legacy systems undergoing modifications to adapt to a service-oriented architecture will design anti-corruption layers to support the transitional period.</td>
<td>Required except pre-bundled COTS products</td>
<td>N/A</td>
</tr>
<tr>
<td>Software Development</td>
<td>The Army will build to the highest abstraction of cloud services, where possible, to include SaaS, PaaS, Database Management as a Service (DBaaS), and so forth, in order to accelerate testing, accreditation and fielding to the Army. Use of hybrid will be by exception and at the approval of the Enterprise Cloud Management Office (ECMO).</td>
<td>Army Cloud Plan</td>
<td>The contractor must build to the highest abstraction of cloud services in order to meet functional, technical, performance and cost goals. These services include commercial SaaS, PaaS, Database Management as a Service, and so forth, in order to accelerate testing, accreditation and fielding to the Army.</td>
<td>N/A</td>
<td>Required</td>
</tr>
<tr>
<td>Software Development</td>
<td>All new software development must use modern software development methodologies (e.g., agile, DevSecOps) to support rapid delivery of standardized, reliable, integrated and secure mission capabilities.</td>
<td>Army Cloud Plan</td>
<td>The contractor must use modern software development methodologies (e.g., agile, DevSecOps) to support rapid delivery of standardized, reliable, integrated and secure mission capabilities.</td>
<td>Optional</td>
<td>Required</td>
</tr>
<tr>
<td>Software Development</td>
<td>All new software acquisitions should use microservices architecture and automation where technically and economically feasible.</td>
<td>Army Cloud Plan</td>
<td>The contractor must use microservices architecture and automation where technically and economically feasible.</td>
<td>Optional</td>
<td>Required</td>
</tr>
<tr>
<td>Software Development</td>
<td>In order to create interoperable, accessible and visible services, all interface information will be published in the Army Data Services Catalog (EDSIC).</td>
<td>Army Data Plan</td>
<td>The contractor must comply with publishing all application programming interface (API) information within the Enterprise Data Services Catalog (EDSIC).</td>
<td>Required</td>
<td>Required</td>
</tr>
</tbody>
</table>

### Security

- **Reference:** DoD Instruction 8500.1; each DoD information system is required to have an Information System Security Program (ISSP) and must implement DoD Risk Management Framework (RMF) governed by DoD Instruction 8110.01, for DoD Information Technology (IT). All cloud instances will inherit RMF controls to the greatest extent allowable by the Authorizing Official.

<p>| Security | Mandatory Implementation of Army Data Standards Services Requirements: (10 April 2020) | Principle D5R1-1.2: Import Data Governance Capabilities Migrating to Army-approved Cloud Environments (1 May 2020) | The contractor must comply with implementation of the DoD Risk Management Framework (RMF) as governed by DoD Instruction 8110.01, for DoD Information Technology (IT). | Required | Required | N/A | N/A | Yes | Yes | Yes | No | Nothing |</p>
<table>
<thead>
<tr>
<th>Security</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Army cloud instances and core Army Future Command (AFC)'s Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance Center (CSSR) as their Cybersecurity Services Provider (CSSP). Exceptions can only be granted by the Army Cyber Combined Enterprise RD&amp;E Program Management Office (P32).</td>
<td>All new and existing applications, systems, or services deemed non-legacy shall be developed, or modified data and functionality through service interfaces (for example, OpenAPI specification). (Mandatory) Implementation of Army Data Standards Services Requirements Memo (10 April 2020), Principle (DS-6).</td>
</tr>
<tr>
<td>The contractor must work with Army Future Command (AFC)'s Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance Center (CSSR) to establish Cyber Security Service Provider (CSSP) services (as required by DoDI 8530 and as described by the Defense Information Systems Agency Computing Security Requirements Guide) for Army applications hosted in commercial cloud.</td>
<td>The contractor must ensure that all new and existing applications, systems, or services deemed non-legacy shall expose their data and functionality through service interfaces (for example, OpenAPI specification).</td>
</tr>
<tr>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>New</td>
<td>Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020)</td>
</tr>
<tr>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Metadata about all Army data assets must be registered in the Army Enterprise Data Services Catalog (EDSC) and comply with DOD Core Metadata Element Sets and International Standards Organization Metadata Elements: requirements (Mandatory) Implementation of Army Data Standards Services Requirements Memo (10 April 2020), Principle (DS-5).</td>
<td>All Army data sources must be developed with built-in data exchange capabilities. Data mapping must also be implemented to increase efficiency and ease of use of data assets as they are being translated or transformed. At a minimum, programs and initiatives are required to comply with Global Force Management Data Initiative; International Standards for Date; Geopolitical Entities, Common (GENC); Joint Communication, Command and Control Exchange Data Model or Resource Description Framework standards and schemes. (Mandatory) Implementation of Army Data Standards Services Requirements Memo (10 April 2020), Principle (DS-5).</td>
</tr>
<tr>
<td>The contractor must ensure that all Army data assets are registered in the Army Enterprise Data Services Catalog (EDSC) and comply with DOD Core Metadata Element Sets and International Standards Organization Metadata Elements: requirements.</td>
<td>The contractor must ensure that all new and existing applications, systems, or services deemed non-legacy shall expose their data and functionality through service interfaces (for example, OpenAPI specification).</td>
</tr>
<tr>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Data management plans must be managed across its lifecycle and captured in a data management plan. (Mandatory) Implementation of Army Data Standards Services Requirements Memo (10 April 2020), Principle (DS-5).</td>
<td>All Army data sources must be developed with built-in data exchange capabilities. Data mapping must also be implemented to increase efficiency and ease of use of data assets as they are being translated or transformed. At a minimum, programs and initiatives are required to comply with Global Force Management Data Initiative; International Standards for data; Geopolitical Entities, Common (GENC); Joint Communication, Command and Control Exchange Data Model or Resource Description Framework standards and schemes. (Mandatory) Implementation of Army Data Standards Services Requirements Memo (10 April 2020), Principle (DS-5).</td>
</tr>
<tr>
<td>Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020).</td>
<td>The contractor must ensure that all new and existing applications, systems, or services deemed non-legacy shall expose their data and functionality through service interfaces (for example, OpenAPI specification).</td>
</tr>
<tr>
<td>N/A</td>
<td>Required</td>
</tr>
</tbody>
</table>
| Data Management Plan.
<table>
<thead>
<tr>
<th>Data</th>
<th>Planning Security Incident Data CSP Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020).</td>
<td>The contractor must utilize government approved controlled source repositories to store all government-funded software development or customization of COTS products.</td>
</tr>
<tr>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>CSF</td>
<td>Once available, procurement of all DoD Information Impact Level (IL) 6 and below Cloud Service Provider (CSP) Offerings will use the Army's Enterprise CSP Reseller contract.</td>
</tr>
<tr>
<td>New</td>
<td>Optimal</td>
</tr>
<tr>
<td></td>
<td>Once available, procurement of all DoD Information Impact Level (IL) 6 and below Cloud Service Provider (CSP) Offerings will use the Army's Enterprise CSP Reseller contract.</td>
</tr>
<tr>
<td>Required, Once Available</td>
<td>Required, Once Available</td>
</tr>
<tr>
<td>CSP</td>
<td>For those CSP Services that exist outside of the Enterprise Reseller contract today, the CSP owner must sign and integrate their AWS Share cloud instances to the Army Cost and Utilization Management Tool, to secure ECMO (a view of all Army CSP resources and spend).</td>
</tr>
<tr>
<td>New</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>All Cloud Service Offerings (CSO) requirements up through DoD Information Impact Level (IL) 6 and below are within scope of the Army Enterprise Cloud Contract vehicle. The only Inter-Process communication allowed is intra-system exchanges or service interface calls over the network.</td>
</tr>
<tr>
<td></td>
<td>Required, Once Available</td>
</tr>
<tr>
<td>Data</td>
<td>All data resides physically within the legal jurisdiction of the United States. If the location of the data is not physically maintained within the legal jurisdiction of the United States, written determination from the Contracting Officer to utilization are not another location is required (AW DFARS 239.7602-23(a)).</td>
</tr>
<tr>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>Security Incident Planning</td>
<td>The Army must adhere to the DoD Cloud Computing Security Requirements Guide version 1 release 3 or superseding versions or releases. (Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020)).</td>
</tr>
<tr>
<td>Required</td>
<td>Required</td>
</tr>
</tbody>
</table>
Security

Contracts shall only be awarded to a cloud service provider that DISA granted a DoD Provisional Authorization (PA), at the level appropriate to the requirement, to deliver the relevant cloud computing model IAW with the DoD CC SRG. The Contractor will ensure that the cloud environment fully complies or exceeds the security requirements for level in the DoD Cloud Security Model SRG. The Contractor will make the environment accessible for a DoD security team to evaluate the environment prior to the placement of any DoD data in the environment and allow for periodic security reviews of the environment during the performance of this contract.

Required Required Required Required Yes No No

Data must be encrypted at rest and in-transit

The contractor shall ensure that all data-at-rest and data in-transit is encrypted utilizing NSA-approved encryption.

Required Required Required Required Yes No No

Cost Management and Reporting

The Contractor shall ensure that all cloud-related costs/price, which include but are not limited to: cost of modernization and migration of applications, Cloud Service Provider (CSP) costs, and cloud Operations and Maintenance (O&M) costs/prices are clearly identified and available for government reporting purposes.

Required Required Required Required Yes No No

Common and Data Services

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Service Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Operating System Vulnerability Scanning</td>
<td>Operating System vulnerability scanning service (e.g., Assured Compliance Assessment Solution (ACAS))</td>
</tr>
<tr>
<td>2 IP Address Management</td>
<td>Planning, tracking, and managing the Internet Protocol (IP) address space used in the cloud environment</td>
</tr>
<tr>
<td>3 Virtual Datacenter Security Stack (VDSS)</td>
<td>All VDSS components and services (e.g. Web Application Firewall, Reverse Proxy, etc.) listed in DISA cloud SRG and SCCA documents, and DoD enclave protection firewall</td>
</tr>
<tr>
<td>4 Key Management</td>
<td>PKI certificate signing, administration, and key management</td>
</tr>
<tr>
<td>5 Network Infrastructure Management and Monitoring</td>
<td>Monitor, manage, and alert on events related to network utilization and availability</td>
</tr>
<tr>
<td></td>
<td>Service</td>
</tr>
<tr>
<td>---</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>6</td>
<td>DDos Protection Service</td>
</tr>
<tr>
<td>7</td>
<td>DNS Hosting, Caching, Recursion</td>
</tr>
<tr>
<td>8</td>
<td>PKI Cert Validation</td>
</tr>
<tr>
<td>9</td>
<td>Network Time</td>
</tr>
<tr>
<td>10</td>
<td>Patch Management</td>
</tr>
<tr>
<td>11</td>
<td>SMTP Relay</td>
</tr>
<tr>
<td>12</td>
<td>Enterprise Directory Services</td>
</tr>
<tr>
<td>13</td>
<td>Federated Access Management</td>
</tr>
<tr>
<td>14</td>
<td>Secure File Transfer Service (SFTP)</td>
</tr>
<tr>
<td>15</td>
<td>Notification Services</td>
</tr>
<tr>
<td>16</td>
<td>Endpoint Monitoring</td>
</tr>
<tr>
<td>17</td>
<td>Remote Privileged Access</td>
</tr>
<tr>
<td>18</td>
<td>Centralized Logging/Auditing</td>
</tr>
<tr>
<td></td>
<td>19</td>
</tr>
<tr>
<td>---</td>
<td>----</td>
</tr>
<tr>
<td>20</td>
<td>Data Dissemination Service</td>
</tr>
<tr>
<td>21</td>
<td>Code Repository</td>
</tr>
<tr>
<td>22</td>
<td>STIG Compliant Virtual Server Templates</td>
</tr>
<tr>
<td>23</td>
<td>License/Software Management</td>
</tr>
<tr>
<td>24</td>
<td>Asset Management Services</td>
</tr>
<tr>
<td>25</td>
<td>Cross Domain Solution (CDS)</td>
</tr>
<tr>
<td>26</td>
<td>CSSP Services</td>
</tr>
<tr>
<td>27</td>
<td>Continuous Integration / Continuous Delivery/Deployment (CI/CD) Tools</td>
</tr>
<tr>
<td>28</td>
<td>Enterprise Data Catalog and Service Registry</td>
</tr>
<tr>
<td>29</td>
<td>Container Platform</td>
</tr>
<tr>
<td>30</td>
<td>Budget and Cost Management</td>
</tr>
<tr>
<td>31</td>
<td>Resource Management Portal</td>
</tr>
</tbody>
</table>
* Note - This listing is current as of 1 May 2020. The number of services is expected to increase as the Army cloud environment matures.

**CLIN SLIN Descriptions**

Cloud Migration, Hosting, and Managed Services Work Breakdown Structure Potential CLIN/SLIN) Descriptions (separately identified & priced) (aligned with PWS)

<table>
<thead>
<tr>
<th>2.6.1 Cloud Migration Support</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2.6.1.1 Migration Analysis:</strong> Price for assessment/detailed analysis of the required effort to migrate to cloud environment</td>
</tr>
<tr>
<td><strong>2.6.1.2 Reengineering:</strong> Price for adjusting code or configuration to ensure Operating Systems and Applications can be supported in target Cloud environment. Includes effort to convert OS to target platform, re-establish interface capabilities, user portal connectivity and access, as well as effort virtualize application or data storage</td>
</tr>
<tr>
<td><strong>2.6.1.2.1 Refactoring:</strong> Price for re-architecting and recoding portions of the application to be compatible with cloud native frameworks/functionality. Includes, for instance, virtualization and conversion to x86 (Optional Detail)</td>
</tr>
<tr>
<td><strong>2.6.1.2.2 Re-platforming:</strong> Price for efforts associated with changes to system software and middleware to adhere to the cloud environment target platform without changing applications core functionality (Optional Detail)</td>
</tr>
<tr>
<td><strong>2.6.1.2.3 Re-hosting:</strong> Price for moving from one hosted environment to another. Includes effort to adjust system API/interfaces (Optional Detail)</td>
</tr>
<tr>
<td><strong>2.6.1.3 Cybersecurity:</strong> Price for security/RMF to achieve cybersecurity compliance and ATO</td>
</tr>
<tr>
<td><strong>2.6.1.4 Application or System Migration:</strong> Priced effort to move or install applications, systems or other components</td>
</tr>
<tr>
<td><strong>2.6.1.5 Data Migration:</strong> Priced Effort to migrate/converge data/databases</td>
</tr>
</tbody>
</table>
2.6.1.6 Initial Provisioning/Configuration: Priced Effort to provision operating environments and configure platform management software

2.6.1.7 Cloud Access Point Fee: Priced Effort to establish Cloud Access Point connection to DISA Network (DoD Network Connectivity)

2.6.1.8 Test and Evaluation: Priced Effort to complete testing to ensure performance criteria can be met

2.6.2 Recurring Hosting

2.6.2.1 Hosting Infrastructure

2.6.2.1.1 Compute: Price for computing resources (vCPU/core, RAM) consumed by operating environments

2.6.2.1.2 Database: Price for database operating environments

2.6.2.1.3 Data Transfer (In/Out): Price data transfer in/out of the network or sent to the systems

2.6.2.1.4 Storage/Backup Storage: Price for cloud storage or back up storage

2.6.2.2 Software Licenses: Price for software licenses that are provided by the cloud provider. This can include, for example, Oracle licenses provided as a part of the cloud operating environment. This does not include, for example, application licenses provided by other vendors that are not part of the cloud offering

2.6.2.3 Cloud Management Licenses: Price for software products including middleware that monitor and manage cloud environment

2.6.2.4 Cloud Services

2.6.2.4.1 Application Management Services (AMS): Price for functional application support (SAP/Oracle applications)

2.6.2.4.2 Cloud Managed Support Services

2.6.2.4.2.1 Monitoring/Server Administration: Priced Effort to monitor and manage servers and operating system
2.6.2.4.2.2 **Database Management/Administration**: Priced Effort to monitor and manage application databases, database administration, and SAP HANA support

2.6.2.4.2.3 **Security/Information Assurance**: Priced Effort associated with ongoing information assurance, security compliance, and Risk Management Framework

2.6.2.4.2.4 **Software Patching and Deployment**: Priced Effort associated with implementing operating system software patches as well as database, middleware, and application patches; generally applicable under PaaS

2.6.2.4.2.5 **Program Management**: Price for project management and oversight. Also includes the preparation of management CDRLs

2.6.2.4.2.6 **Training**: Price to develop education/training materials or conduct training on cloud related principals and techniques

2.6.2.4.2.7 **Transition**: Price to develop a transition plan, support a transition to another MSP provider, or support a transition to another cloud or an on-premise solution

2.6.2.4.2.8 **Continuous Improvement**

2.6.2.4.2.8.1 **Process Automation**: Effort to develop and maintain tools and scripts used to improve deployment, elasticity, and cloud management

2.6.2.4.2.8.2 **Architecture Reengineering**: Effort, usually provided under managed services, to optimize cloud infrastructure