### Policy and PWS Language

<table>
<thead>
<tr>
<th>Subject Area</th>
<th>Policy</th>
<th>Policy Reference/Source</th>
<th>1a) Migrating to the Cloud</th>
<th>1b) New SW Development in the Cloud</th>
<th>2a) Follow-on contracts related to service and management</th>
<th>2b) Cloud Identity, Enterprise Solutions</th>
<th>New Contracts</th>
<th>Orders Against Existing Contracts</th>
<th>Existing Contracts</th>
<th>EDSL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud</td>
<td>All commercial cloud usage must be reported via the Army Portfolio Management System (APMS) per data EXORD 689-20. All Army system/applications developed in, operated on, and hosted in the commercial cloud must be cataloged in the DoD FedRamp Data Catalog (DFC). The Army will not duplicate common service and data services that are accredited in cloud, to include the components of the DoD Service Catalog (DSC). If a service is required that is not yet available in cloud, the Application/Owner must work with the Enterprise Cloud Management Office (ECMO) to define the service, and then the ECMO will work with the Army Data Center to procure the service. The Army will use the DoD FedRamp Data Catalog (DFC) to identify available services and APIs.</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Use of Enterprise Services</td>
<td>The contractor must use Army Enterprise Cloud Plan to contract services, data services, and all cloud services.</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Use of Enterprise Services</td>
<td>The contractor must use Army Data Plan to identify available data services and APIs.</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Modernization/Migration</td>
<td>The contractor must comply with mandatory software development methodologies (e.g., DevSecOps) to support rapid delivery of functional, technical, performance and cost effective services.</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Software Development</td>
<td>The contractor must use Cloud Computing Security Requirements Guide (DoD 8519.01) for Cloud Computing Security Controls (CCSC) to ensure cloud services and data services are protected and are operationally sustainable and in accordance with DoD 8530 and as described by the DISA Cloud Computing Standard (CSEC).</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Software Development</td>
<td>The contractor must comply with mandatory software development methodologies (e.g., DevSecOps) to support rapid delivery of functional, technical, performance and cost effective services.</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Software Development</td>
<td>The contractor must comply with mandatory software development methodologies (e.g., DevSecOps) to support rapid delivery of functional, technical, performance and cost effective services.</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Security</td>
<td>The contractor must comply with mandatory software development methodologies (e.g., DevSecOps) to support rapid delivery of functional, technical, performance and cost effective services.</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Data</td>
<td>The contractor must comply with mandatory software development methodologies (e.g., DevSecOps) to support rapid delivery of functional, technical, performance and cost effective services.</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

#### Building Blocks

- **Cloud**: \( \text{EXORD 689-20} \)
- **Use of Enterprise Services**: \( \text{Army Cloud Plan} \)
- **Modernization/Migration**: \( \text{Army Cloud Plan} \)
- **Software Development**: \( \text{Army Cloud Plan} \)
- **Security**: \( \text{Army Data Plan} \)
- **Data**: \( \text{Army Data Plan} \)

#### Contract Actions

- **New Contracts**: \( \text{N/A} \)
- **Orders Against Existing Contracts**: \( \text{N/A} \)
- **Existing Contracts**: \( \text{N/A} \)
- **ESDL**: \( \text{N/A} \)

---

### Additional Notes

- **Policy and PWS Language**: Required
- **Data**: Required
- **Security**: Required
- **Cloud**: N/A
- **Use of Enterprise Services**: N/A
- **Software Development**: N/A
- **Modernization/Migration**: N/A
- **Architecture Planning and Description of Services**: N/A
- **Cloud Computing Strategy and Roadmap**: N/A

---

### Army Cloud Plan

- **Legacy systems undergoing modernization to adopt a service-oriented architecture should design and deploy services and interfaces in a reusable manner. Pre-built COTS products are excluded.**
- **Cloud Native Principles**: N/A
- **Data Services**: N/A
- **Security**: N/A
- **Legacy systems undergoing modernization to adopt a service-oriented architecture should design and deploy services and interfaces in a reusable manner. Pre-built COTS products are excluded.**
- **Cloud Native Principles**: N/A
- **Data Services**: N/A
- **Security**: N/A

---

### Army Data Plan

- **The contractor must ensure that legacy systems undergoing modernization to adopt a service-oriented architecture should design and deploy services and interfaces in a reusable manner. Pre-built COTS products are excluded.**
- **Cloud Native Principles**: N/A
- **Data Services**: N/A
- **Security**: N/A

---

### Security

- **The contractor must ensure that all new and existing applications, systems, or services that are controlled and exposed through service interfaces be designed to be consumable from external sources and plan and design to be able to expose the interface to developers.**
- **Security Plan**: N/A
- **Data**: N/A

---

### Use of Enterprise Services

- **Cloud**: N/A
- **Use of Enterprise Services**: N/A
- **Modernization/Migration**: N/A
- **Software Development**: N/A
- **Security**: N/A
- **Data**: N/A

---

### Software Development

- **Cloud**: N/A
- **Use of Enterprise Services**: N/A
- **Modernization/Migration**: N/A
- **Software Development**: N/A
- **Security**: N/A
- **Data**: N/A

---

### Data

- **Cloud**: N/A
- **Use of Enterprise Services**: N/A
- **Modernization/Migration**: N/A
- **Software Development**: N/A
- **Security**: N/A
- **Data**: N/A
## Common and Data Services

### Service Name

<table>
<thead>
<tr>
<th>Service Description</th>
<th>1 Operating System Vulnerability Scanning</th>
<th>2 IP Address Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning, tracking, and managing the Internet Protocol (IP) address space used in the cloud environment</td>
<td>Operating System vulnerability scanning service (e.g., Assured Compliance Assessment Solution (ACAS))</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Service Description</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>-------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Virtual Datacenter Security Stack (VDSS)</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Key Management</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Network Infrastructure Management and Monitoring</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>DDoS Protection Service</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>DNS Hosting, Caching, Recursion</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>PKI Cert Validation</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Network Time</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Patch Management</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>SMTP Relay</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Enterprise Directory Services</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Federated Access Management</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Secure File Transfer Service (SFTP)</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Notification Services</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Endpoint Monitoring</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Remote Privileged Access</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Centralized Logging/Auditing</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Security Information and Event Management (SIEM) and Log Analytics</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Data Dissemination Service</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Code Repository</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>STIG Compliant Virtual Server Templates</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>License/Software Management</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Asset Management Services</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Cross Domain Solution (CDS)</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>CSSP Services</td>
<td></td>
</tr>
</tbody>
</table>

**Virtual Datacenter Security Stack (VDSS)**

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.

**Key Management**

PKI certificate signing, administration, and key management.

**Network Infrastructure Management and Monitoring**

Monitor, manage, and alert on events related to network utilization and availability.

**DDoS Protection Service**

Protects applications in the cloud environment from Distributed Denial of Service (DDoS) attacks.

**DNS Hosting, Caching, Recursion**

DNS lookup for cloud-based applications and hierarchical DNS management delegated to mission owners.

**PKI Cert Validation**

Online Certificate Status Protocol (OCSP) responder to validate if PKI certificates are valid or revoked.

**Network Time**

Cybersecurity mandated accurate time source for DoD systems hosted in the cloud.

**Patch Management**

Patch repositories for common operating system patch files.

**SMTP Relay**

Simple Mail Transport Protocol (SMTP) based email relay.

**Enterprise Directory Services**

Privileged administrative user and non-person entity Identity, Credential, and Access Management (ICAM) (e.g., Active Directory [AD], Lightweight Directory Access Protocol [LDAP])

**Federated Access Management**

User Identity, Credential, and Access Management (ICAM) (e.g., EAMS-A, SAML Services)

**Secure File Transfer Service (SFTP)**

Securely transfer large files to the cloud environment.

**Notification Services**

Alerting and notification (e.g., Short Message Service [SMS])

**Endpoint Monitoring**

Protects computing endpoints from malware and other cyber security threats (e.g., Host Based Security Service [HBSS])

**Remote Privileged Access**

Secure administrative access from the Internet or DODIN to DoD servers in secure cloud enclaves.

**Centralized Logging/Auditing**

Consolidated aggregation point for receiving and storing logs from systems and applications in the cloud environment.

**Security Information and Event Management (SIEM) and Log Analytics**

Identifies and categorizes security related incidents and events.

**Data Dissemination Service**

Accelerates and consolidates data for transfer utilizing secure network tunnels.

**Code Repository**

Code repository for source code configuration management to support a software factory.

**STIG Compliant Virtual Server Templates**


**License/Software Management**

Operating System (OS) level license management.

**Asset Management Services**

Discover and track assets such as resources, licensed software, etc. within the cloud environment.

**Cross Domain Solution (CDS)**

Automatically move appropriately vetted files between security classification levels.

**CSSP Services**

Standardized tools & processes to meet cloud cyber security requirements; primarily provided by C5ISR to cArmy tenants. Collaboration with cArmy cloud services ops team.
Continuous Integration / Continuous Delivery/Deployment (CI/CD) Tools
Tools to enable the CI/CD pipeline (e.g., tools similar to the capabilities provided in DI2E.net)

Enterprise Data Catalog and Service Registry
Data and service listing for data and service management and automated data processing

Container Platform
Enabling container runtime services (e.g., container orchestration)

Budget and Cost Management
Provides cloud cost and budget information to mission owners

Resource Management Portal
Portal to manage compute and store resources

* 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)

**2.6.1 Cloud Migration Support**

2.6.1.1 Migration Analysis: Price for assessment/detailed analysis of the required effort to migrate to cloud environment

2.6.1.2 Reengineering: 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

2.6.1.2.1 Refactoring: 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)

2.6.1.2.2 Re-platforming: 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)

2.6.1.2.3 Re-hosting: Price for moving from one hosted environment to another. Includes effort to adjust system API/interfaces (Optional Detail)

2.6.1.3 Cybersecurity: Price for security/RMF to achieve cybersecurity compliance and ATO

2.6.1.4 Application or System Migration: Priced effort to move or install applications, systems or other components
2.6.1.5 Data Migration: Priced Effort to migrate/converge data/databases

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