### Policy and PWS Language

<table>
<thead>
<tr>
<th>Subject Area</th>
<th>Policy</th>
<th>Policy Reference/Source</th>
<th>PWS Language</th>
<th>Building Blocks</th>
<th>Contract Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud</td>
<td>All commercial cloud usage must be reported via the Army Financial Management System (AFMS) per data EXORD 069-20</td>
<td>EXORD 069-20</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use of Enterprise Services</td>
<td>All Army system/applications developed in, maintained in, or hosted in the commercial cloud must provide application programming interfaces (APIs) and data services. The Army will not duplicate common service or data services that are accredited in the cloud, to include the components of the DoD Services. The cloud computing architecture (CCA) for a service is required that it not yet available in the cloud, the Application Owner must work with the CIO/G6 Cloud Computing Governance Office (CCGO) to deploy a service taxonomy, as defined in DoDI 8505.01.</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modernization/Migration</td>
<td>The Army will modernize applications applying Cloud-Native Design Principles, which will prioritize the use of SaaS as a Service (SaaS) and Platform as a Service (PaaS) (to include container technology) over infrastructure as a Service (IaaS) models to reduce total cost of ownership.</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Development</td>
<td>The Army will build or procure software capabilities to support rapid delivery of standardized, reliable, integrated and secure mission capable applications.</td>
<td>N/A</td>
<td></td>
<td></td>
<td></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 microservice-capable applications.</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Development</td>
<td>All new software development must use modern software development methodologies (e.g., agile, DevSecOps) to support the development of standardized, reliable, integrated and secure mission capabilities.</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Development</td>
<td>In order to create interoperable, accessible and visible services, all inter-service interfaces will be governed by the Army Enterprise Data Services Catalog (EDSC).</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>All Army cloud instances will use Army Future Command (AFC)’s Cloud Control, Governance, Surveillance and Resilience Center (C2GSR) as their Cybersecurity Service Provider (CSP). Exception can only be granted by the Army Cyber Center (ARCYBER) or the Chief Information Officer (CIO/G6).</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td>All new and existing applications, systems, or services that store, process, or transmit data and functionally through service interfaces (e.g., OpenAPI) must also be published to the DoD Data Catalog and be compliant with technical requirements.</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td>All service interfaces, without exception, must be designed to be consumable from external services and planning to be able to expose the interface to developers.</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Building Blocks**: N/A
- **Contract Actions**: Required

---

*Mandatory: N/A
Required: N/A
COTS: N/A
Yes: N/A
No: N/A

*Migration Plan for Army to use SaaS and PaaS as a Service (SaaS) and Platform as a Service (PaaS) (to include container technology) over infrastructure as a Service (IaaS) models to reduce total cost of ownership.

*Catalog or inventory of common services will be available within the app.

*System design document

*Architecture Drawing and Description of Salaries

*Software Development Plans

*Architecture Design and Description of Salaries

*Plan and Schedule for migration to EDCS

*Army Cloud Plan

*Catalog or inventory of common services will be available within the app.

*System design document

*Architecture Drawing and Description of Salaries

*Software Development Plans

*Architecture Design and Description of Salaries

*Plan and Schedule for migration to EDCS

*Army Cloud Plan

*Catalog or inventory of common services will be available within the app.

*System design document

*Architecture Drawing and Description of Salaries

*Software Development Plans

*Architecture Design and Description of Salaries

*Plan and Schedule for migration to EDCS
Common and Data Services

**Service Name**

1. Operating System Vulnerability Scanning
2. IP Address Management

**Service Description**

1. Operating System vulnerability scanning service (e.g., Assured Compliance Assessment Solution (ACAS))
2. Planning, tracking, and managing the Internet Protocol (IP) address space used in the cloud environment
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.


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.