

1

2 Army Enterprise Application/System

3 Modernization and Migration to

4 Commercial Cloud Statement of

5 Objectives (SOO)

6



7

8 Army Enterprise Cloud Management

9 Agency (ECMA)

10

11 April 2021

12

13

Contents

1. Overview	3
2. Background	3
3. Scope	3
4. Period and Place of Performance	3
5. Data Storage, Data Rights, and Data Ownership	4
6. Application Modernization and Migration Into Commercial Cloud (and Optional Application Maintenance) Objectives and Requirements	4
6.1. Objective 1: Conduct Application Assessment	5
6.2. Objective 2: Application Modernization and Migration into commercial cloud/cARMY	6
6.3. Objective 3: Operations, Maintenance and Continual Enhancement of Applications (Optional as Required).....	7
6.4. Objective 4: Training (Optional as required).....	8
7. Constraints	8
7.1. Program Management	8
7.2. Software Licensing (Option).....	8
7.3. Cyber Security Requirements	9
7.4. Transition In Requirements.....	9
7.5. Transition Out Requirements.....	10
7.6. Operations Security (OPSEC), Training, Clearance and Access	10
8. Service Delivery Summary.....	13
9. cARMY Common Shared Services List.....	13

1. Overview

This document describes the Army's objectives and requirements to provide an Enterprise scale contractual vehicle or agreement to modernize and migrate Army applications/systems (henceforth referred to as "applications") and data into commercial cloud environments.

2. Background

In accordance with the Army's Cloud Plan¹, the Army's ability to master the application of cloud computing is a critical enabler in the pursuit to operationalizing data. As such, the Army requires an Enterprise scale capability to modernize and migrate applications and data into commercial cloud. The preponderance of Army applications will migrate into cARMY, which is the Army's Enterprise Cloud Environment, managed by Headquarters Department of the Army (HQDA)/Office of the Chief Information Office (OCIO) Enterprise Cloud Management Agency (ECMA). cARMY currently offers authorized and operational common shared services in Amazon Web Services (AWS) and Microsoft Azure at Department of Defense (DoD) Information Impact Level (IL) 2, 4 and 5, with contracts/plans in place to develop common shared services at IL 6. Exceptions to migrating into cARMY will be considered by the Army when there is a strong business case to do so, an example of which might be through use of a Software as a Service (SaaS) offering not available in cARMY. Prior to migrating into cARMY or any commercial cloud, Applications must be modernized, using Cloud Native Design principles, to take advantage of the full benefits of commercial cloud.

3. Scope

The scope of this Statement of Objectives (SOO) includes performing deep application assessments and modernizing and migrating applications into DoD authorized IL 2,4,5 and 6 commercial cloud environments. The application assessments shall allow the Army to make an intelligent business decision as to whether and how to refactor, replatform, recode or replace each application to best meet mission requirements. Once the Government decides on a modernization strategy for a particular application, the contractor shall execute the strategy to modernize and migrate the application into the commercial cloud. For planning purposes, the contractor shall assume the Army will modernize and migrate to commercial cloud between 50-150 applications each year. The scope of this effort also includes optional capabilities to operate and continually enhance Army Applications once they have migrated into the cloud.

4. Period and Place of Performance

The base Period of Performance will be one (1) year from date of award with two (2) one (1) year options.

Place of performance will be primarily in Contractor provided facilities, with the expectation of regular meetings on Government premises at Fort Belvoir, VA, or other Government owned or leased facilities. The Government requires that the Contractor currently maintains a Secret facility

¹ <https://api.army.mil/e2/c/downloads/2020/09/11/81bb912e/the-army-cloud-plan-2020-final2.pdf>

clearance and functional Secret Internet Protocol Router (SIPR) Network workspace where Secret classified work can be performed.

5. Data Storage, Data Rights, and Data Ownership

The Contractor must physically maintain all data solely on equipment located within the legal jurisdiction of the United States IAW DFARS 239.7602-2(b). All data, including but not limited to documents, administrative data, support data, and billing data, transmitted via the system or maintained in the system shall reside at all times in data processing and storage equipment located in the United States or in data processing and storage equipment of which the operation and maintenance are subject only to the laws of the United States. Data transmitted must only be subject to disclosure pursuant to U.S. Federal law and not the laws of any other jurisdiction or foreign nation. All DoD information/data placed or created by DoD users in a Cloud Service Provider's (CSP) Cloud Service Offering (CSO) is owned by the DoD, the Mission Owner, and/or their Information Owner. The CSP has no rights to the DoD's information/data. For more information on data storage, data rights, and data ownership requirements refer to Section 5.2, Legal Considerations, in the DoD Cloud Computing Security Reference Guide (SRG) v1r3.

The Government shall retain unlimited rights to all development and automation performed and all data, Infrastructure-as-Code (IaC) or Configuration as Code (CaC) or processes created under this contract. This would not include code, processes, or automation that the Army might subscribe to that are commercially available under Commercial Use Rights and/or Government Purpose Rights.

The Data Rights clauses in the basic contract are invoked for all data generated in the performance of this Order. For non-commercial scripts, automation and technical data deliverables under this task order, Unlimited Rights are required. See clauses DFARS 252.227-7013, 252.227-7014, and 252.227-7015.

The Government shall retain unlimited rights of all user data/information/knowledge provided to, created/developed in, loaded/transitioned to, or hosted in/by the contractor, CSP, tenant, multiple CSP, multiple tenants, CSO, vendor IT infrastructure, hosting environment, system(s). This includes rights to logs, scans, analytics, and other data, conducted by the contractor, CSP, or tenant, on their IT infrastructure, hosting environment, system(s) or prototype process. The Government retains the right to request full copies of this data at any time.

The contractor shall fill out Appendix A: Data Rights Table, as part of their proposal.

6. Application Modernization and Migration Into Commercial Cloud (and Optional Application Maintenance) Objectives and Requirements

The Army requires a capability to modernize applications and migrate them into the commercial cloud, mainly within the AWS and/or Microsoft Azure cARMY environments. For all applications migrating into cARMY, the contractor shall use cARMY Enterprise Common Shared Services, shown in section 9.0. The contractor shall use all DoD Secure Cloud Computing Architecture (SCCA) components when developing, migrating and hosting Army

systems/applications in the commercial cloud. When developing a proposed to-be cloud architecture for a particular application, the contractor shall identify their proposed solution's software licensing requirements. The contractor shall only propose Open Source with a secure supply chain and/or universally accessible Commercial Off the Shelf (COTS) licensable software, or Government off the Shelf (GOTS), based on Open Standards². All Cloud Service Offering (CSO) requirements up through DoD Information Impact Level (IL) 6 that are within scope of the Army Enterprise Cloud Agreement, known as the Cloud Account Management Optimization (CAMO) agreement, shall be purchased off that vehicle. The contractor shall register all cloud instances into the cARMY cost and utilization management tool with any CSP procurement. Cloud instances shall be registered into cARMY's management tool within 15 business days of procurement. The Contractor shall ensure that all cloud-related costs/price, which include but are not limited to: cost of modernization and migration of applications, and cloud Operations and Maintenance (O&M) costs/prices are clearly identified and available for government reporting purposes.

The following is a list of the Army's objectives and requirements for each Army application modernized and migrated under this solicitation:

6.1. Objective 1: Conduct Application Assessment

The contractor shall provide a thorough assessment of an application's composition to determine the proper modernization and migration methods necessary to host the in the commercial cloud/cARMY and capitalize on cloud services. The contractor shall propose modernizing the application applying Cloud Native Design Principles and shall prioritize use of SaaS and Platform as a Service (PaaS) over Infrastructure as a Service (IaaS). Areas of focus for the Application Assessment Report shall include, but are not limited to:

- **Application Architecture:** Analyze the application structure (presentation layer, application layer, data/layer repository) and the ability to virtualize it as well as identify the integration of the common services required along with the native cloud services to be used.
- **Data:** Analyze the applications' data schema, data transfer and database requirements and identify potential alternatives to meet the Government's objectives for reduced cost or improved data accessibility.
- **Performance:** Analyze the application's performance and throughput requirements to identify equivalent performance requirements are met with the post migrated, cloud-based, application. Specifically analyze the impact of changes in network latency on application performance.
- **Availability:** Analyze the application's Recovery Time Objective (RTO) and Recovery Point Objective (RPO) and data replication requirements.

² Open Standards defined as follows: be created by domain experts (not Standard Development Organization [SDO] staff); be developed under and internationally respected, open process (i.e., be open for public review and debate); be easy to access and adopt; have allowed anyone affected by the standard to contribute to the development of it; not have hidden patents to scare implementers; have the ability to implement the standard baked in (i.e., OASIS standards must be verified by multiple Statements of Use); and be safe for governments to endorse.

- **Integration:** Analyze the application integration requirements and determine whether any modifications are required to the hosting environment to include those required to support legacy system interfaces.
- **Operations:** Analyze the operational and maintenance needs of the application and whether it can be supported by the hosting environment.
- **Cybersecurity Risk Assessment:** Analyze the application's cybersecurity risks including code STIG and design flaws that would prevent the application from operating securely in the new target hosting environment.
- **Cost & Schedule:** Analyze the application's modernization, migration and hosting cost as well as schedule to migrate.
- **Target CSP Environment:** Analyze whether the application is more suited to AWS and/or Microsoft Azure, or another cloud service provider.
- **Licensing:** Analyze if and how licensing associated with application will be impacted by proposed modernization and migration.

The results of the analysis shall allow the Army to make an informed business decision as to how to modernize the existing application to meet mission requirements and utilize cARMY common shared services as appropriate. The contractor may also propose a greenfield approach, which would replace the existing application entirely. Improvements and recommendations shall only be implemented at the discretion and direction of the Government and shall fall under Objective 2.

6.2. Objective 2: Application Modernization and Migration into commercial cloud/cARMY

The contractor shall modernize each application as directed by the Government, which will be informed by Objective 1. The contractor shall ensure that the modernization fully complies or exceeds the security requirements for the appropriate impact level per the DoD Cloud Security Model SRG. Prior to modernization and migration, the contractor shall deliver an application transition and cutover plan to include a RACI Chart illustrating stakeholder responsibilities. The contractor shall ensure that the application modernization and migration is compliant with Agile/Development Security and Operations (DevSecOps) methodologies. The contractor shall maximize use of the Army's Coding Resources and Transformation Environment (CReATE) tools and services. The contractor shall modernize applications with a focus on human/user experience design.

In addition, the contractor shall:

- Collaborate with the Government to establish application access controls
- Determine and integrate the required common services for the application
- Conduct unit testing and user acceptance testing (UAT) to include providing test scripts/test reports to the Government PMO
- Assist the Information System Security Engineer (ISSE) and/or the Information System Security Manager (ISSM) in conducting A&A to demonstrate that the Risk Management Framework (RMF) requirements have been met.

• Migrate the applications to the cARMY production environment or other commercial cloud environment based on a Government “go-live” decision.

The contractor shall provide the Government with an Application Migration Report after migration is complete to document the list of the changes made to the application and corresponding rationale for each change and the methodology used to accomplish the items (e.g., interfaces, dependencies, etc.) defined in the Analysis Report. The application Migration Report shall include results from the application test. It is expected that the Assessment Report will be used as a foundation for the Migration Report.

In accordance with Army Federal Acquisition Regulation Supplement (AFARS) Part 5139 Appendix HH, the contractor shall ensure that legacy systems undergoing modifications to adapt to a service-enabled architecture will design anti-corruption layers to support the transitional period. The contractor shall ensure that all new and existing applications, systems, or services deemed non-legacy shall expose their data and functionality through service interfaces (e.g., OpenAPI specification). The contractor shall ensure that all service interfaces, without exception be designed to be consumable from external sources and must plan and design to be able to expose the interface to developers. The contractor shall ensure that all Army data assets are registered in the Army Enterprise Data Service Catalog (EDSC) and comply with Dublin Core Metadata Element Sets and International Standards Organization Metadata Registries requirements. The contractor shall ensure that All Army data sources are developed with built-in data exchange capabilities. Data mapping shall also be implemented to increase efficiency and ease of use of data assets as they are being translated or transformed. At a minimum, the contractor shall comply with Global Force Management Data Initiative; International Standards for dates; Geopolitical Entities, Names and Codes, Common (GENC); Joint Consultation, Command and Control Exchange Data Model; or Resource Description Framework standards and schemas. The contractor shall utilize government approved centralized source code repositories to store all government funded software development or customization of COTS products.

6.3. Objective 3: Operations, Maintenance and Continual Enhancement of Applications (Optional as Required)

Using Agile/DevSecOps principles, the contractor shall provide application operations, maintenance, and continual enhancement activities such as, (but not limited to):

- Patch Application, Platform and Operating System as appropriate
- Fix Production Defects
- Fix Cybersecurity Vulnerabilities
- Provide other Application-level CSSP Support: non inherently-governmental application cybersecurity services as defined in DoD Instruction 8530.01 *Cybersecurity Activities Support to DoD Information Network Operations* to Protect, Detect, Respond, and Sustain applications and data in the commercial cloud

The contractor shall ensure that all current application architectures are maintained in a government repository and that all software used by each application are appropriately licensed. The Government shall furnish the root cloud account or the appropriate role / IAM as Government Furnished Equipment (GFE) to the contractor to manage. The Contractor shall ensure at all times

that the Government has highest access rights to the root cloud account (e.g., if they change passwords, Government gets the new password).

The contractor shall employ continuous integration and outreach to ensure customer satisfaction with the changes and updates to the application.

The contractor shall propose an application Service Level Agreement (SLA), which shall minimally include the following metrics:

- Availability: defines system/service uptime and accessibility
- Reliability: measured against mean time between failures (MTBF) and mean time to repair (MTTR) or return to service
- Recovery Point Objective: permissible data loss within a service or group of services
- Recovery Time Objective: permissible time to recover to operations

The contractor shall provide a defined SLA end-to-end implementation approach to include SLA definitions, reporting, and remediation of SLA deficiencies. The contractor and government will mutually agree upon the final SLA. The contractor shall clearly identify where government dependencies exist. The contractor shall also clearly identify where CSP dependencies exist.

The contractor shall request government approval for any planned service interruptions.

6.4. Objective 4: Training (Optional as required)

The contractor shall provide training on how to operate the migrated application in the cloud. The Government desires the contractor to use online training to the maximum extent possible. The contractor shall provide all training material in original and editable formats, to the Government. Training should include, but is not limited to, Standard Operating Procedures (SOPs), automation scripts and processes, security and performance documentation, listings of current deficiencies, incident ticket data, etc.

7. Constraints

7.1. Program Management

The contractor shall have a single point of contact for coordination with the Government Program Management Office; successfully integrate and coordinate all activity needed to execute all other Objectives and requirements within this SOO; provide corrective action plans, timely identification of issues, and effective management of subcontractors; ensure it provides the appropriate management and resources to ensure overall success of the program is achieved, including maintaining schedule, program reviews, test events, training, deployment to designated locations, sustainment, quality, program management, and risk management; maintain professional and ethical behavior of all contractor personnel.

7.2. Software Licensing (Option)

The Government intends to leverage existing Army Licensing Agreements, Joint Enterprise License Agreements (JELAs), and/or Enterprise Licensing Agreements (ELAs) to purchase licenses required for each application, with a goal of minimizing the purchasing of software

licenses under this Enterprise Application Modernization and Migration contract. However, the contractor shall retain the ability to procure software licenses directly under this contract when the Government deems it necessary to do so. All licenses purchased under this contract will be owned by the Government. The Government reserves the right to buy required software licenses outside of this contract and provide them as Government Furnished Equipment (GFE).

7.3. Cyber Security Requirements

The Contractor shall maintain administrative, technical, and physical safeguards and controls required for the security level and services being provided in accordance with (IAW) the Cloud Computing Security Requirements Guide (SRG) Version 1 Release 3 (v1r3), or latest version. The solution must meet security standards and controls specified in DoDI 8500.01 (Cybersecurity) and 8510.01 (RMF). IL6 Cloud services developed under this order will be DoD Security Requirements Guide (SRG) IL6 assessed and authorized under the Director of National Intelligence (DNI) Intelligence Community Directive (ICD 503) and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4.

- The contractor will be responsible for generating and providing RMF required authorization related documentation and artifacts to the cARMY Information System Security Owner (ISO) and Manager (ISSM). The contractor will support the Assessment & Authorization (A&A) process for cARMY. The contractor will support the DoD Cloud Authorization Process, creating any required documentation to obtain a Cloud Service Offerings (CSO) and/or Cloud Service Provider (CSP) Provisional Authority (PA).
- The contractor will be responsible for performing Cybersecurity vulnerability scans and addressing all findings in accordance with DoD and Army directives and policies
- The contractor will conduct Information Assurance Vulnerability Management (IAVM) Monitoring and Response activities, to include development and production of all necessary documentation to support these activities
- The contractor will work with the Government's chosen Cyber Security Service Provider (CSSP) to establish CSSP services (as required by DoDI 8530 and as described by the DISA Cloud Computing Security Requirements Guide) for Army applications hosted in commercial cloud
- The contractor shall ensure that all data-at-rest and data in-transit is encrypted utilizing NSA-approved encryption
- The contractor will comply with the DoD Secure Cloud Computing Architecture (SCCA)
- The contractor must adhere to the DoD Cloud Computing Security Requirements Guide version 1 release 3 (or superseding versions or releases). Contractors must provide security incident response plans. Updates to the plans are required on an annual basis or when a significant change occurs to the technical or operational environment.

7.4. Transition In Requirements

The contractor shall enter into Associate Contractor Agreements (ACA) with applicable third-party integrators and other stakeholders after contract award for any portion of the contract requiring joint participation in the accomplishment of the requirement. The agreements shall

include the basis for sharing information, data, technical knowledge, expertise and/or resources essential to this effort, which shall ensure the greatest degree of cooperation to meet the terms of the contract. The Government will provide specific names of contractors to the contractor.

ACAs shall include, but not limited to, the following general information:

- a) Identify the associate contractors and their relationships.
- b) Identify the program involved and the relevant Government contracts of the associate contractors.
- c) Describe the associate contractor interfaces by general subject matter.
- d) Specify the categories of information to be exchanged or support to be provided.
- e) Include the expiration date (or event) of the ACA.
- f) Identify potential conflicts between relevant Government contracts and the ACA; include agreements on protection of proprietary data and restrictions on employees.

The contractor is not relieved of any contract requirements or entitled to any adjustments to the contract terms because of a failure to resolve a disagreement with an associate contractor.

Liability for the improper disclosure of any proprietary data contained in or referenced by any ACA shall rest with the parties to the ACA and not the Government. All costs associated with the ACAs are included in the negotiated cost of this contract. ACAs may be amended as required by the Government during the performance of this contract. The contractor shall submit copies of all ACAs to the Contracting Officer.

7.5. Transition Out Requirements

The contractor shall deliver a comprehensive transition-out plan that provides a detailed description of the transfer of full assumption of duties to a potential follow-on contractor. Transition out plans must be updated on an annual basis and submitted to the government for approval. The contractor will follow a similar process to the Transition In, but as the incumbent.

7.6. Operations Security (OPSEC), Training, Clearance and Access

1. Anti-Terrorism (AT) Level I Training. All contractor employees, including subcontractor employees, requiring access to Army installations, facilities, and controlled-access areas shall complete AT Level I awareness training within 7 calendar days after the contract start date or effective date of incorporation of this requirement into the contract, whichever is applicable. The contractor shall submit certificates of completion for each affected contractor employee and subcontractor employee, to the Contracting Officer Representative (COR) or to the contracting officer, if a COR is not assigned, within 7 calendar days after completion of training by all employees and subcontractor personnel. AT Level I awareness training is available at the following website: <http://jko.jten.mil>.

2. Contractor and all associated sub-contractor's employees shall provide all information required for background checks to meet installation access requirements to be accomplished by installation Provost Marshal Office, Director of Emergency Services or Security Office. Contractor workforce must comply with all personal identity verification requirements (FAR clause 52.204-9, Personal Identity Verification of Contractor Personnel) as directed by DOD, HQDA and/or local policy. In addition to the changes otherwise authorized by the changes clause of this contract, should the

Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in contractor security matters or processes.

a. For contractors requiring Common Access Card (CAC). Before CAC issuance, the contractor employee requires, at a minimum, a favorably adjudicated National Agency Check with Inquiries (NACI) or an equivalent or higher investigation in accordance with Army Directive 2014-05. The contractor employee will be issued a CAC only if duties involve one of the following: (1) Both physical access to a DoD facility and access, via logon, to DoD networks on-site or remotely; (2) Remote access, via logon, to a DoD network using DoD-approved remote access procedures; or (3) Physical access to multiple DoD facilities or multiple non-DoD federally controlled facilities on behalf of the DoD on a recurring basis for a period of 6 months or more. At the discretion of the sponsoring activity, an initial CAC may be issued based on a favorable review of the FBI fingerprint check and a successfully scheduled NACI at the Office of Personnel Management.

b. For contractors that do not require CAC but require access to a DoD facility or installation. Contractor and all associated sub-contractors employees shall comply with adjudication standards and procedures using the National Crime Information Center Interstate Identification Index (NCIC-III) and Terrorist Screening Database (TSDB) (Army Directive 2014-05/AR 190-13), applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by government representative), or, at OCONUS locations, in accordance with status of forces agreements and other theater regulations.

3. US based contractor employees and associated sub-contractor employees shall make available and receive government provided area of responsibility (AOR) specific AT awareness training as directed by AR 525-13. Specific AOR training content is directed by the combatant commander with the unit ATO being the local point of contact.

4. The contractor and all associated sub-contractors shall brief all employees on the local iWATCH program (training standards provided by the requiring activity ATO). This local developed training will be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the COR. This training shall be completed within 7 calendar days of contract award and within 7 calendar days of new employees commencing performance with the results reported to the COR NLT 7 calendar days after contract award.

5. All contractor employees with access to a government info system must be registered in the ATCTS (Army Training Certification Tracking System) at commencement of services, and must successfully complete the DOD Information Assurance Awareness prior to access to the IS and then annually thereafter.

6. The contractor shall develop an OPSEC Standing Operating Procedure (SOP)/Plan within 90 calendar days of contract award, to be reviewed and approved by the responsible Government OPSEC officer. This plan will include a process to identify critical information, where it is located, who is responsible for it, how to protect it and why it needs to be protected. The contractor shall implement OPSEC measures as ordered by the commander. In addition, the contractor shall have an identified certified Level II OPSEC coordinator per AR 530-1.

7. Per AR 530-1 Operations Security, the contractor employees must complete Level I OPSEC Awareness training. New employees must be trained within 30 calendar days of their reporting for duty and annually thereafter.

8. All contractor employees and associated sub-contractor employees must complete the DoD IA awareness training before issuance of network access and annually thereafter. All contractor employees working IA/IT functions must comply with DoD and Army training requirements in DoDD 8570.01, DoD 8570.01-M and AR 25-2 within six months of appointment to IA/IT functions.

9. Per DoD 8570.01-M, DFARS 252.239.7001 and AR 25-2, the contractor employees supporting IA/IT functions shall be appropriately certified upon contract award. The baseline certification as stipulated in DoD 8570.01-M must be completed upon contract award.

10. For all contractors with security clearances. Per AR 381-12 Threat Awareness and Reporting Program (TARP), contractor employees must receive annual TARP training by a CI agent or other trainer as specified in 2-4b.

11. The Contractor shall comply with any future training requirements issued by the Government that are deemed necessary for this contract.

12. Retrieving Identification Media. Contractor shall retrieve all identification media, including vehicle decals, from employees who depart for any reason before the contract expires, e.g., terminated for cause, retirement.

13. Listing of Employees. Contractor will maintain a current listing of employees assigned to this project or task. The list will include employee's name, social security number, and level of security clearance. The list will be validated and signed by the company Facility Security Officer (FSO) and provided to the contracting officer, prior to the contract kickoff date. Updated listings will be provided when an employee's status or information changes.

14. Freedom of Information Act Program (FOIA). Contractor will comply with DoD Regulation 5400.7/Army Supplement, DoD Freedom of Information Act Program, requirements. The regulation sets policy and procedures for the disclosure of records to the public and for marking, handling, transmitting, and safeguarding Controlled Unclassified Information (CUI) material.

15. Reporting Requirements. Contractor will comply with specified Army reporting requirements. Contractor personnel will report to an appropriate authority (Contracting Officer or Security Police) any information or circumstances of which they are aware may pose a threat to the security of DoD personnel, contractor personnel, resources, and classified or unclassified defense information. Contractor employees will be briefed by their immediate supervisor upon initial on-base assignment and as required thereafter.

16. Physical Security. Areas occupied by contractor employees will comply with base Operations Plans/instructions for FPCON procedures, Random Antiterrorism Measures (RAMS) and local search/identification requirements. Contractor will safeguard all Government property including controlled forms provided for contractor use. At the close of each work period, Government training equipment, ground aerospace vehicles, facilities, support equipment, and other valuable materials will be secured.

17. Controlled/Restricted Areas. Contractor will implement local base procedures for entry to Army controlled/restricted areas where contractor personnel will work. Fort Belvoir requires special Army access badges to gain entrance to the Office of the CIO Fort Belvoir Buildings.

8. Service Delivery Summary³

Delivery or Required Services	Performance Standard	Acceptable Quality Level	Surveillance Method
Test Code Coverage	The contractor shall ensure any new software (SW) code being developed is supported by automated tests	Minimum of 90% test coverage of all code	COR/Product Manager continuous surveillance
Security	The contractor shall ensure the SW code base and documentation meet the security controls identified in NIST SP 800-53 REV4.	Code submitted must be free of medium- and high-level static and dynamic security vulnerabilities prior to pushes to production	COR/Product Manager continuous surveillance
User-Centered Design	The contractor shall ensure all Application/System User Interfaces utilize user-centered design, and that usability testing and other research methods with end users are conducted at regular intervals throughout the development process (not just at the beginning or end)	Artifacts from usability testing and/or other research methods with end users are available at the end of every applicable feature, IAW the vendor's research plan	COR/Product Manager continuous surveillance
Application/System ATO	The contractor shall ensure that Application X receives and maintains its ATO through automated security scanning and compliance with RMF protocols.	95% of all security artifacts and processes are documented and validated by the Authorizing Official;	COR / Product Manager continuous surveillance

440

9. cARMY Common Shared Services List

The table below lays out the cARMY Common Shared Services list, with services available in each environment (AWS/Azure) today.

Service Number	Service Name	Service Description
Foundational Services		

³ For another example, go to [technology-budgeting/handbook.md at master · 18F/technology-budgeting · GitHub](#)

1	Operating System Vulnerability Scanning	Operating System vulnerability scanning service (e.g., Assured Compliance Assessment Solution [ACAS])
2	IP Address Management	Planning, tracking, and managing the Internet Protocol (IP) address space used in the cloud environment
3	Reverse Proxy	Provide a reverse proxy capability to handle access requests from client systems
4	Next Generation Firewall	Provide a Next Generation Firewall which meets or exceeds DoD Secure Cloud Computing Architecture (SCCA) Functional Requirements Document (FRD) specifications (e.g., provide a capability that can distinguish and block unauthorized application layer traffic, inspection of SSL/TLS communication traffic, interfaces to conduct ports, protocols, and service management (PPSM) activities, full packet capture (FPC) or cloud service equivalent FPC capability for recording and interpreting traversing communications, etc.).
5	Web Application Firewall (WAF)	Provide a capability to inspect and filter application layer conversations based on a predefined set of rules (including HTTP) to identify and block malicious content
6	Firewall Management System	Provides a mechanism for privileged users to manage firewalls to include collection and analysis of security and metrics information
7	Cloud Access Security Broker (CASB)	Provides security policy enforcement services which combine and interject enterprise security policies as the cloud-based resources are accessed.
8	Key Management	PKI certificate signing, administration, and key management
9	Network Infrastructure Management	Configure and manage underlying network infrastructure

10	DDoS Protection Service	Protects applications in the cloud environment from Distributed Denial of Service (DDoS) attacks
11	Global Transport Management	Manage global data transport systems to include transport within and out the Army's authorization boundaries and across security classification levels.
Enterprise Services		
12	DNS Hosting, Caching, Recursion	DNS lookup for cloud-based applications and hierarchical DNS management delegated to mission owners
13	PKI Cert Validation	Online Certificate Status Protocol (OCSP) responder to validate if PKI certificates are valid or revoked
14	Network Time	Cybersecurity mandated accurate time source for DoD systems hosted in the cloud
15	Patch Management	Patch repositories for common operating system patch files.
16	SMTP Relay	Simple Mail Transport Protocol (SMTP) based email relay
17	Identity and Access Management (IdAM)	Privileged, user, device, and non-person entity Identity and Access Management (IdAM) (e.g., Active Directory [AD], Lightweight Directory Access Protocol [LDAP], Credential Provisioning, Federation, Secrets Management)
18	Secure File Transport Services	Securely transfer large files to the cloud environment
19	Notification Services	Alerting and notification (e.g., Short Message Service [SMS])

20	Endpoint Monitoring	Protects computing endpoints from malware and other cyber security threats (e.g., Host Based Security Service [HBSS])
21	Remote Privileged Access	Secure administrative access from the Internet or DODIN to DoD servers in secure cloud enclaves.
22	Centralized Logging/Auditing	Consolidated aggregation point for receiving and storing logs from systems and applications in the cloud environment
23	Security Information and Event Management (SIEM) and Log Analytics	Identifies and categorizes security related incidents and events
24	Data Dissemination Service	Accelerates and consolidates data for transfer utilizing secure network tunnels.
Enabling Services		
25	Code Repository	Code repository for source code configuration management to support IaC
26	STIG Compliant Virtual Server Templates	A library which stores DISA Security Technical Implementation Guide (STIG) compliant virtual machine template images
27	Software License Management Service	Software license management services
28	Asset Management Services	Discover and track assets such as resources, licensed software, etc. within the cloud environment
29	CSSP Services	Standardized tools & processes to meet cloud cyber security requirements
30	Continuous Integration / Continuous Development (CI/CD) Tools	Tools to enable the CI/CD pipeline (e.g., tools similar to the capabilities provided in DI2E.net)
31	Enterprise Data Catalog and Service Registry	Data and service listing for data and service management and automated data processing
32	Container Platform	Enabling container runtime services (e.g., container orchestration)

33	Application Programming Interface (API) Management	Service that creates, publishes and manages API interfaces throughout its lifecycle
Business Services		
34	Budget and Cost Management	Provides cloud cost and budget information to mission owners
35	IT Services Management (ITSM)	Provides services to continually improve IT service strategy across design, transition, and operation. This includes IT user request and fulfillment workflow and visualization.
36	Demand Management	Provides a capacity management capability to assist with understanding, anticipating, and influencing customer demand for IT services.
37	IT Business Management (ITBM)	Provides a service to align business goals with the application portfolio to assist with business requirements planning, resource allocation, and portfolio value evaluation
38	IT Operations Management (ITOM)	Provides a service to manage IT infrastructure and service health, events, performance, optimization, provisioning, configuring, capacity, and process management.
Managed Infrastructure		
39	Resource Management Portal	Portal to manage compute and store resources

444

Service Category	Service Definition
Foundational Services	Foundational Services are composed of the underlying infrastructure required to host and operate Army applications in a commercial cloud environment.
Enterprise Services	Enterprise Services are composed of application level services which directly interface with Army at the operating system level or higher to provide required services in the commercial cloud environment.
Enabling Services	Enabling Services are composed of tools and applications which facilitate modern software lifecycle and application management.
Business Services	Business Services are composed of tools and applications which inform business decisions and provide data to optimize the cloud environment from a financial perspective.
Managed Infrastructure Services	Managed Infrastructure Services are composed of tools and applications which provide an interface for authorized Army users to manage compute, storage, and other cloud services.

445

446

DRAFT

Appendix A: Data Rights Table

The Government has unrestricted rights to all technical data and software delivered under this project, to include deliverables such as reports, training materials, software, and software manuals, unless identified in the following table. All data created, ingested, derived from or migrated from Government sources or processed by the software identified in the following table is owned by the Government.

Item No	Technical Data or Computer Software to be Furnished	Basis for Assertion	Asserted Rights Category	Name of Organization Asserting Restrictions	Milestone # Affected

The following table identifies applicable rights categories, rights criteria, and permitted uses within and by third parties outside of the Government for reference:

Rights Category	Applies to These Types of TD or CS	Rights Criteria	Permitted Uses Within the Government	Permitted Uses by Third Parties Outside the Government ¹
Unlimited Rights (UR)	Noncommercial TD and CS	Developed exclusively at Government expense, and certain types of data (e.g., FFF, OMIT, CSD)	All uses; no restrictions	
Government Purpose Rights (GPR)	Noncommercial TD and CS	Developed with mixed funding	All uses; no restrictions	For "Government Purposes" only; no commercial use ¹
Limited Rights (LR)	Noncommercial TD only	Developed exclusively at private expense	Unlimited; except may not be used for manufacture	Emergency repair or overhaul ²
Restricted Rights (RR)	Noncommercial CS only	Developed exclusively at private expense	Only one computer at a time; minimum backup copies; modification ³	Emergency repair/overhaul; certain service/maintenance contracts ^{1,2}
Specifically Negotiated License Rights	Any/all TD and CS—including commercial TD and CS	Mutual agreement of the parties; use whenever the standard categories do not meet both parties' needs	As negotiated by the parties; however, must not be less than LR in noncommercial TD and must not be less than RR in noncommercial CS (consult with legal counsel as other limits apply)	
SBIR Data Rights	Noncommercial TD and CS	All TD or CS generated under an SBIR contract	The equivalent of Unlimited Rights (UR) in OMIT and FFF data; the equivalent of Limited Rights (LR) in all other delivered TD; the equivalent of Restricted Rights (RR) in CS	
Commercial TD License Rights	Commercial TD only	TD related to commercial items (developed exclusively at private expense) ⁴	The equivalent of Unlimited Rights (UR) in OMIT and FFF data; the equivalent of Limited Rights (LR) in all other delivered TD	
Commercial CS Licenses	Commercial CS only	Any commercial CS or CS documentation	As specified in the commercial license customarily offered to the public ⁵	

*<https://www.dau.mil/cop/mosa/DAU%20Sponsored%20Documents/Data%20Rights%20Focus%20Sheet%20final.pdf>