

Policy and PWS Language

Subject Area	Policy	Policy Reference/Source (AR, DFARS, AFARS, DOD, etc.)	PWS language	Building Blocks			Contract Actions				CDRL
				1a) Migrating to the Cloud	1b) New SW Development in the Cloud	2) Follow-on contracts related to common services and management	3) Cloud Hosting, use of Enterprise solutions	New Contracts	Orders Against Existing Contracts	Existing Contracts	
Cloud	All commercial cloud usage must be reported into the Army Portfolio Management System (APMS) per data EXORD 009-20	EXORD 009-20	N/A								
Use of Enterprise Services	All Army systems/applications developed in, migrated to and hosted in the commercial cloud will use cArmy Enterprise common services and data services. The Army will not duplicate common services or data services that are accredited in cArmy, to include the components of the DoD Secure Cloud Computing Architecture (SCCA). If a service is required that is not yet available in cArmy, the Application/System Owner must work with the Enterprise Cloud Management Office (ECMO) before any development of that service occurs (or any dollars are obligated towards the development). A list of the currently available (as of 1 May 2020) 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: www.cloud.army.mil .	EXORD 009-20: 3.D.5.G. (U) DIRECT THE ENTERPRISE CLOUD MANAGEMENT OFFICE (ECMO) TO DEVELOP A PLAN TO CONSOLIDATE EXISTING CLOUD INSTANCES TO THE GREATEST POSSIBLE EXTENT, AND WITHOUT SIGNIFICANT IMPACT TO ONGOING OPERATIONS, TO GAIN VISIBILITY AND CONTROL OF ARMY CLOUD MIGRATIONS NLT 01 JAN 2020.	The contractor must use cArmy 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: www.cloud.army.mil	Required	Required	N/A	N/A	Yes	No	No	Migration Plan or Strategy to use the common services
Use of Enterprise Services	Existing cloud common services will be consolidated into cArmy 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 onboard their applications into cArmy and reduce the duplicity of services across the Army.	EXORD 009-20: 3.D.5.G. (U) DIRECT THE ENTERPRISE CLOUD MANAGEMENT OFFICE (ECMO) TO DEVELOP A PLAN TO CONSOLIDATE EXISTING CLOUD INSTANCES TO THE GREATEST POSSIBLE EXTENT, AND WITHOUT SIGNIFICANT IMPACT TO ONGOING OPERATIONS, TO GAIN VISIBILITY AND CONTROL OF ARMY CLOUD MIGRATIONS NLT 01 JAN 2020.		N/A	N/A	Required	N/A	Yes	No	No	Catalog or Inventory of common services utilized within the app.

Modernization/Migration	<p>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 toil and overhead of maintaining Information Technology (IT) systems. Use of IaaS will be by exception and at the approval of the Enterprise Cloud Management Office (ECMO). According to the Cloud Native Computing Foundation, "cloud native technologies empower organizations to build and run scalable applications in modern, dynamic environments such as public, private, and hybrid clouds. Containers, service meshes, micro-services, immutable infrastructure, and declarative APIs exemplify this approach. These techniques enable loosely coupled systems that are resilient, manageable, and observable. Combined with robust automation, they allow engineers to make high-impact changes frequently and predictably with minimal toil." *</p>	Army Cloud Plan	<p>The contractor must modernize applications migrating to commercial cloud 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).</p>	Mandatory	N/A	N/A	N/A	Yes	No	No	System design document
Modernization/Migration	<p>Legacy systems undergoing modifications to adapt to a service-enabled architecture should design anti-corruption layers** to support the transitional period. Pre-bundled COTS products are excluded.</p>	Army Cloud Plan	<p>The contractor must ensure that legacy systems undergoing modifications to adapt to a service-enabled architecture will design anti-corruption layers to support the transitional period.</p>	Required except pre-bundled COTS products	N/A	N/A	N/A	Yes	No	No	Architecture Drawing and Description of Solution
Software Development	<p>The Army will build to the highest abstraction of cloud services, where possible, to include SaaS, PaaS, Database Management as a Service, and so forth, in order to accelerate testing, accreditation and fielding to the Army. Use of IaaS will be by exception and at the approval of the Enterprise Cloud Management Office (ECMO).</p>	Army Cloud Plan	<p>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.</p>	N/A	Required	N/A	N/A	Yes	No	No	Architecture Drawing and Description of Solution
Software Development	<p>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.</p>	Army Cloud Plan	<p>The contractor must use modern software development methodologies (e.g., agile, DevSecOps) to support rapid delivery of standardized, reliable, integrated and secure mission capabilities.</p>	Optional	Required	N/A	N/A	Yes	No	No	Software Development Plans
Software Development	<p>All new software acquisitions should use microservices architecture and automation where technically and economically feasible.</p>	Army Cloud Plan	<p>The contractor must use microservices architecture and automation where technically and economically feasible.</p>	Optional	Required	N/A	N/A	Yes	No	No	Software Development Plan and Architecture
Software Development	<p>In order to create interoperable, accessible and visible services, all interface information will be published in the Army Enterprise Data Services Catalog (EDSC).</p>	Army Data Plan	<p>The contractor must comply with publishing all application programming interface (API) information within the Enterprise Data Services Catalog (EDSC)</p>	Required	Required	N/A	N/A	Yes	Yes	No	Plan and Schedule for publishing to EDSC
Security	<p>Reference DoD Instruction 8580.1; each DoD information system is required to have an Information System Security Manager (ISSM) and must implement DoD Risk Management Framework (RMF) governed by DoD Instruction 8510.01, for DoD Information Technology (IT). All cloud instances will inherit RMF controls to the greatest extent allowable by the Authorizing Official.</p>	<p>Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020), Principle DSR-1. 2. Impact-level Guidance for Data Migrating to Army-approved Cloud Environments (1 May 2020) 3. Authorization Guidance for IT Capabilities Migrating to Army-approved Cloud Environments. (1 May 2020)</p>	<p>The contractor must comply with implementation of the DoD Risk Management Framework (RMF) as governed by DoD Instruction 8510.01, for DoD Information Technology (IT).</p>	Required	Required	N/A	N/A	Yes	Yes	No	

Security	All Army cloud instances will use Army Future Command (AFC)'s Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance Center (C5ISR) as their Cybersecurity Service Provider (CSSP). Exceptions can only be granted by the Army Cyber Command (ARCYBER) or the Chief Information Officer (CIO)/G6.	New	The contractor must work with Army Future Command (AFC)'s Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance Center (C5ISR) to establish Cyber Security Service Provider (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.	Required	Required	Required	N/A	Yes	Yes	Yes	
Data	All new and existing applications, systems, or services deemed non-legacy shall expose their data and functionality through service interfaces (for example, OpenAPI specification). (Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020), Principle DSR-6)	Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020)	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).	Required	Required	N/A	N/A	Yes	No	No	
Data	All service interfaces, without exception, must be designed to be consumable from external sources and must plan and design to be able to expose the interface to developers. (Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020), Principle DSR-7)	Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020)	The contractor must 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.	Required	Required	N/A	N/A	Yes	No	No	
Data	Metadata about all Army data assets must be registered in the Army Enterprise Data Service Catalog (EDSC) and comply with Dublin Core Metadata Element Sets and International Standards Organization Metadata Registries requirements. (Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020), Principle DSR-3.)	Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020)	The contractor must 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.	Required	Required	N/A	N/A	Yes	No	No	
Data	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 dates; Geopolitical Entities, Names and Codes, Common (GENC), Joint Consultation, Command and Control Exchange Data Model; or Resource Description Framework standards and schemas. (Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020), Principle DSR-4)	Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020)	The contractor must ensure that All Army data sources are 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 dates; Geopolitical Entities, Names and Codes, Common (GENC), Joint Consultation, Command and Control Exchange Data Model; or Resource Description Framework standards and schemas.	Optional	Required	N/A	N/A	Yes	No	No	
Data	Data 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 DSR-5)	Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020),	N/A	Required	Required	N/A	N/A	Yes	Yes	No	Data Management Plan

Data	All custom software or customized COTS software written by the Army or developed with Army funding will be centrally controlled and made available to all DoD, IC and inter-agency partners within the approved Army source code repositories on the Unclassified, Secret, and Top Secret networks in accordance with Army Directive 2018-26 (Enabling Modernization Through the Management of Intellectual Property) (Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020), Principle DSR-8)	Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020),	The contractor must utilize government approved centralized source code repositories to store all government funded software development or customization of COTS products.	Required	Required	Required	N/A	Yes	No	No
Data	There will be no other form of Inter-Process communication allowed: no direct linking, no direct reads of another data store, no shared-memory model, and no back-doors whatsoever. The only Inter-Process communication allowed is intra-system data exchanges or service interface calls over the network. All other requests or methods require CIO approval (Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020), Principle DSR-9)	Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020),	The contractor must ensure that there will be no other form of Inter-Process communication allowed: no direct linking, no direct reads of another data store, no shared-memory model, and no back-doors whatsoever. The only Inter-Process communication allowed is intra-system data exchanges or service interface calls over the network.	Optional	Mandatory	N/A	N/A	Yes	No	No
CSP	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. Exceptions to this policy include programs funded by Military Intelligence Program (MIP)/National Intelligence Program (NIP) monies. Other exceptions can only be granted by the ECMO. As contract options expire, existing CSP service contracts will also be migrated to the Army's Enterprise CSP reseller contract.	New	All Cloud Service Offering (CSO) requirements up through DoD Information Impact Level (IL) 6 that are within scope of the Army Enterprise Cloud Contract Vehicle will be purchased off that vehicle.	Required, Once Available	Required, Once Available	Required, Once Available	Required, Once Available	Yes	No	No
CSP	For those CSP Services that exist outside of the Enterprise reseller contract today, the CSP owner must align and integrate their AWS/Azure cloud instances to the cArmy Cost and Utilization Management Tool, to ensure ECMO can view all Army CSP resources and spend.	New	The contractor will register all cloud instances into the cArmy cost and utilization management tool with any CSP procurement. Cloud instances will be registered into cArmy's management tool within 15 business days of procurement.	Required	Required	Required	Required	Yes	No	No
Data	All data will reside 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 authorize use of another location is required IAW DFARS 239.7602-2(b).	DFARS 239.7602-2(b)	The Contractor must maintain all data within the legal jurisdiction of the United States IAW DFARS 239.7602-2(b).	Required	Required	Required	Required	Yes	No	No
Security Incident Planning	The Army must adhere to the DoD Cloud Computing Security Requirements Guide version 1 release 3 (or superseding versions or releases). IAWS DFARS 239.7604	DoD Cloud Computing Security Requirements Guide (DoD CC SRC) Version 1 Revision 3, Section 6.5.1, IAW DFARS 239.7604	The contractor must adhere to the DoD Cloud Computing Security Requirements Guide version 1 release 3 (or superseding versions or releases). In particular, 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.	Required	Required	Required	Required	Yes	No	No

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.	DoD Cloud Computing Security Requirements Guide (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 periodical security reviews of the environment during the performance of this contract.	Required	Required	Required	Required	Yes	No	No	
Security	Data must be encrypted at rest and in-transit	CNSSP 15, AR 25-2	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	Cost Report (Cost Summary Data Report 1921, 1921-5) and CWBS Dictionary	EXORD 009-20	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	Cost/price Report

Parent topic: [APPENDIX - HH Table Of Contents](#)