THE U.S. ARMY

CLOUD PLAN

October 2022

army.mil/ecma

facebook.com/armycio

twitter.com/armycio

linkedin.com/company/armycloud

instagram.com/armycio

The data-centric Army employs advanced lethality, survivability, and tempo – empowers Leaders and Soldiers with the right information at the right time to gauge risk, optimize combat power, fully employ national means, and attain decision dominance at all echelons.

FOREWORD

As acknowledged in the 2021 Army Digital Transformation Strategy (ADTS) and 2019 Army Modernization Strategy, developing and leveraging the cloud is the foundation for Army modernization. To maintain information superiority and deliver decision dominance in accordance with the U.S. CIO Federal Cloud Computing Strategy,[1] and the DoD Software Modernization Strategy the total Army must leverage cloud-smart and cloud-native digital technologies to forge a sustainable, strategic path to the Army of 2030. The data-centric Army employs advanced lethality, survivability, and tempo – empowers Leaders and Soldiers with the right information at the right time to gauge risk, optimize combat power, fully employ national means, and attain decision dominance at all echelons.

Building on the vision of the previous Army Cloud Plan 2020, the Army Cloud Plan 2022 provides a strategic approach to the actions the Army will take to scale and operationalize the cARMY cloud in support of the Warfighter. This approach extends from rationalization and optimization of data centers in the continental United States (CONUS) to tactical deployments outside the continental United States (OCONUS) in a way that is secure, resilient, and scalable. The Army's commitment to reducing its data center footprint, centralizing operations to accelerate modernization to the cloud, and adopting innovative digital technologies are key enablers of the ADTS.

The Army Cloud Plan 2022 lays out the following seven strategic objectives: Expand Cloud; Implement Zero Trust Architecture; Enable Secure, Rapid Software Development; Accelerate Data-Driven Decisions; Enhance Cloud Operations; Develop the Cloud Workforce; and Provide Cost Transparency and Accountability. The plan includes the roadmap and metrics to measure progress that will enable the Army to achieve these objectives, implement a global architecture, meet sustainable, strategic goals, and maintain decision dominance over U.S. near-peer adversaries.

DR. RAJ G. IYER

Chief Information Officer (CIO)
U.S. Army

MR. PAUL B. PUCKETT III

Director, Enterprise Cloud Management Agency (ECMA)
U.S. Army

[1] https://cloud.cio.gov/strategy/

STRATEGIC INTENT

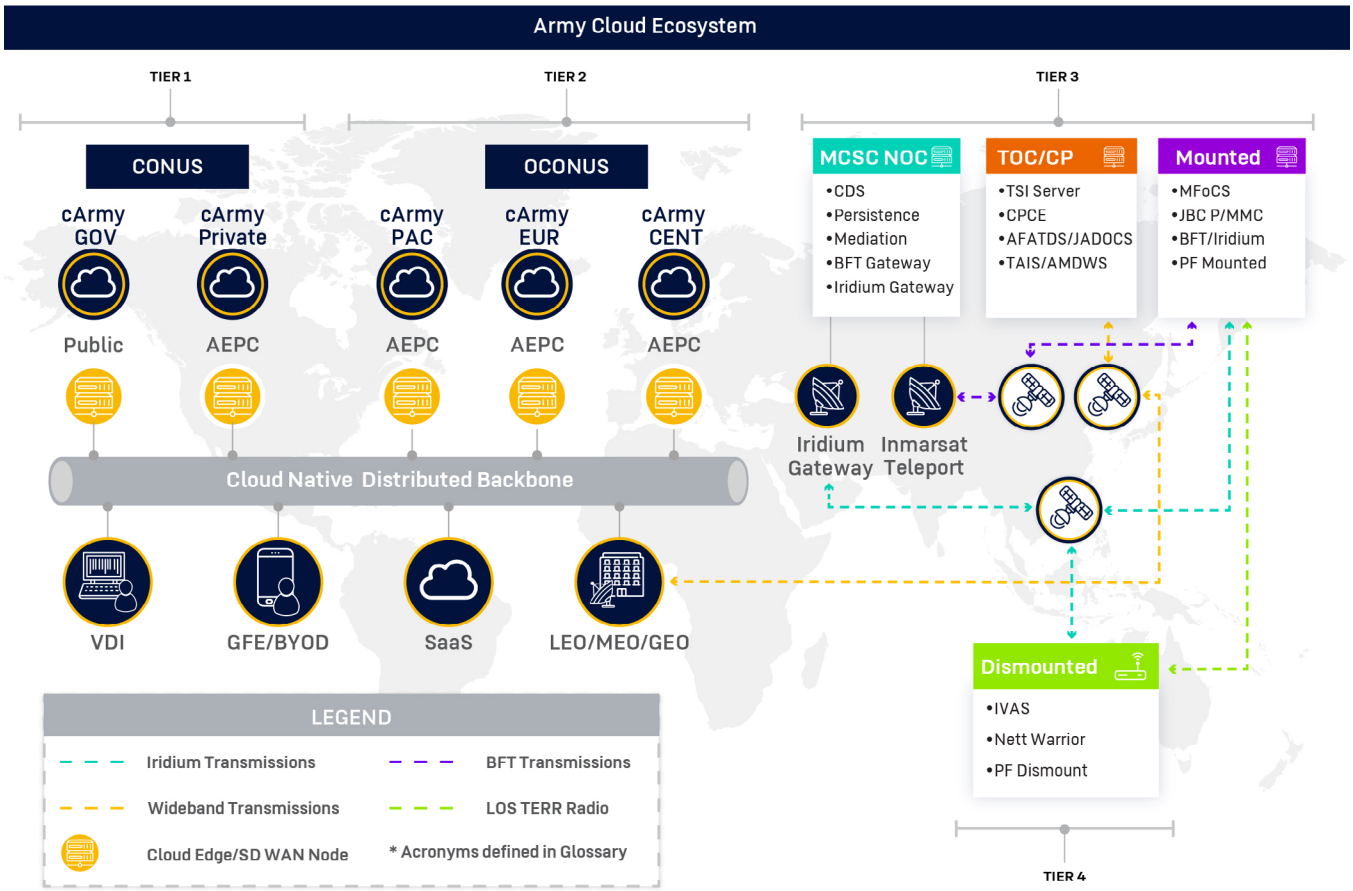
The Army has made significant progress towards its vision and strategy for cloud, and many of the core principles of the Army Cloud Plan 2020 remain steadfast, including: **"The Army must adapt its processes to be more agile, its network to be more resilient, its hybrid public and private cloud environments to be more elastic, IT software design and fielding approaches to be more cloud native, and organization structures and training to be more effective at information warfare."**[2] The Enterprise Cloud Management Agency (ECMA) and its partners successfully established the Army's multi and hybrid cloud ecosystem known as cARMY that provides common cloud shared services, global connectivity and required Cybersecurity Service Provider (CSSP) services for all Army applications, systems and data hosted in the cloud. cARMY general-purpose cloud is the directed hosting environment for all Army cloud activities aligned to the Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) design patterns.[3] For all Software as a Service (SaaS) design patterns, cARMY serves as the broker of connectivity and common cloud services to secure and scale its use across the Total Army. To enable continuous improvement and transformation of the Army, the Army Cloud Plan 2022 identifies new strategic objectives to continue Army-wide cloud adoption, reduce barriers to cloud migration, and engage at every echelon to educate and inform customers on their journey to cloud. Each strategic objective includes a roadmap that details how the Army will execute across the different lines of effort and how it will be measured by defined performance metrics to achieve success.

This includes exploring and incorporating commercial cloud service offerings, and expanding to a global hybrid cloud, with cARMY as an anchor, to an ecosystem of private clouds including those that are OCONUS and support the tactical edge. In addition, the Army will develop innovative solutions around the utilization of colorless transport through a global cloud infrastructure to allow for direct integration with the tactical cloud. This will involve incorporating software-defined wide area networks (SD-WAN), utilizing commercial Satellite communications including Low / Medium / Geosynchronous Earth Orbit (LEO / MEO / GEO), and implementing a zero trust architecture (ZTA), among others, with target environments on-premises, as well as mounted and dismounted solutions. This future Army Cloud Ecosystem, detailed in **Figure 1**, will enable the strategic optimization of the networks connecting Army customers globally and reducing the complexity of networking configurations across the Department of Defense Information Network - Army

[2] Army Cloud Plan 2020

[3] With the exception of Headquarters, Department of the Army (HQDA) G-2 authorities as the required Title 50 Cloud Service Provider for the Army to provide a cloud environment that supports Army Intelligence requirements.

Figure 1. Army Cloud Ecosystem Vision



(DoDIN-A). The Army Cloud Plan activities are fully synchronized with and complementary to the lines of effort in the Army Unified Network Plan (AUNP) established in 2021 since the cloud is an extension of the DODIN-A. While the AUNP focuses on unifying and modernizing transport across the tactical and enterprise networks, the Cloud Plan is focused on delivering cloud-native services and other common services to the unified network.

In order to maximize the value of a globally accessible cloud infrastructure including cost savings from cloud, the Army must continue to develop cloud-native applications designed to thrive within modern architectures. This will reduce the overhead of maintaining technology stack components and focus attention on mission-enabling application and data services. In addition, as the Army continues to scale and operationalize its Development, Security, and Operations (DevSecOps) practices, the Army will move towards providing environments that reduce toil and technical debt abstracting away infrastructure complexity so developers can focus on creating innovative software that supports and enhances mission capabilities as well as enhance the user experience. This, combined with zero trust (ZT) principles and use of Application Programming Interfaces (APIs), will enable secure data exchange at speed, allowing the Army to execute its mission on an ever-evolving digital battleground.

Finally, the Army Cloud Plan 2022 will advance the Army's goal of reducing its twelve enduring data centers down to five by 2028 and converging hundreds of installation processing nodes worldwide. To accomplish this goal, the Army must not just move select applications to the cloud, but fully rationalize all applications at a data center, and migrate them to either cARMY (preferred) or to an identified Army enduring data center.

STRATEGIC OBJECTIVES (SOs)

SO 1: EXPAND CLOUD

While cARMY currently delivers CONUS based enablement and modernization for the Army, the Army must now expand this value into the tactical and edge cloud domains. OCONUS, Tactical and Edge cloud environments will be enabled with the expansion of cARMY leveraging commercial and private hybrid cloud IaaS and PaaS solutions in accordance with the Department of Defense (DoD) OCONUS Cloud Strategy.[4] To support global and multi-domain operations, cARMY will expand to create an ecosystem that extends cloud to include all tiers of operation:

1. **Tier 1:** The broadest level of operations targeted at meeting the Army's strategic outcomes; shows how the Army operates its entire global cloud, including commercial and private clouds.
2. **Tier 2:** Operations targeted at meeting the Army's operational outcomes; focused on how the Army operates regional cloud capabilities. This could include commercial and private clouds.
3. **Tier 3:** Operations targeted at meeting the Army's tactical outcomes; focused on how the Army operates cloud at command, tactical edge, and strategic node echelons.
4. **Tier 4:** Operations targeted at the network of operational sensors at all service echelons, in support of data-driven decisions for real-time outcomes.

This SO requires that the Army unify its networks to create a global network, necessitates that cARMY support common shared services for each tier, and that the Army continue consolidating disparate clouds into the cARMY cloud ecosystem. In accordance with the Army Unified Network Plan 2021,[5] the Army will optimize its use of a global Wide Area Network (WAN) to establish a Cloud Native Distributed Backbone as referenced in 3.2.1.1. of this document.

LINES OF EFFORT

Data Center Optimization

Though many Army mission critical systems, applications, and data have moved to cARMY within the commercial cloud, there are still a large number of Army applications that were designed for, and reside in, on-premises data centers. While the goal is to modernize and migrate these applications to cARMY, there are use cases where these applications best serve the mission by remaining on-premises in a private cloud. To support these applications, existing Army data centers will be consolidated into strategically located on-premises **Army Enterprise Private Clouds (AEPCs)** that are extensions of existing commercial cloud resources and global transport capabilities. These AEPCs will meet all five characteristics of cloud infrastructure through on-demand self-service, resource pooling, rapid elastic scaling, metered services of compute, and storage resources with broad network access. This will require the Army to strategically invest in commodity and high-performance infrastructure to

[4] https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-OCONUSCloudStrategy.pdf
[5] https://api.army.mil/e2/c/downloads/2021/10/07/d43180cc/army-unified-network-plan-2021.pdf

> **The Army must extend its cloud capabilities using commercial transport and ZT principles to OCONUS locations, to include Denied, Disconnected, Intermittent, or Limited (D-DIL) environments.**

include those offered by hyper-scaled Cloud Service Providers (CSPs).

Tasks:

- Deploy an application discovery tool at selected Army data centers and utilize the Enterprise Decision Analytics Framework (EDAF) tool to inform prioritization and rationalization of application modernization and migration to cloud
- Identify the systems and applications that must remain in on-premises data centers to inform AEPC optimization efforts
- Define AEPC enduring sites including the minimum number of data centers required, the hardware (compute/storage) requirements for those applications, and how fast consolidation can be achieved
- Based on the infrastructure requirements, optimize and standardize AEPC hardware to support cARMY's private cloud extension, including incorporating hyperscale CSP hardware into the hardware lifecycle
- Configure communication to cARMY to consume common services for private cloud extensions

Regional OCONUS Cloud Extension

To support transport and services to the tactical networks, the Army must extend its cloud capabilities using commercial transport and ZT principles to OCONUS locations, to include Denied, Disconnected, Intermittent, or Limited (D-DIL) environments. This is critical to be able to provide data, services, and capabilities to the tactical edge and achieve an information advantage for the warfighter.

Tasks:

- Architect, test, and integrate OCONUS cARMY regions utilizing the commercial cloud backbone
- Architect, test, and deploy OCONUS private cloud solutions for datacenters
- Architect, test, and deploy a standard tactical cloud solution that can provide services in a disconnected state, but also sync with cARMY when connected

Enterprise Common Shared Services

The ECMA established cARMY common shared services for the following environments:

- **cARMY-U** – Operational Unclassified environments covering impact levels two through five (IL2-IL5)
- **cARMY-S** – Operational Secret environments covering Impact Level Six (IL6)
- **cARMY-X** – Research and scientific development Unclassified environments covering IL2-IL5
- **cARMY-XS** – Research and scientific development Classified environments covering IL6

The HQDA G-2 established the Army Military Intelligence Cloud Computing Service Provider (AC2SP) common shared services for the following environments:

- **AC2SP-U** – Operational -Unclassified environments covering Army Intelligence IL2 requirements.
- **AC2SP-S** – Operational Secret environments covering Army Intelligence IL6 requirements.
- **AC2SP-TS** – Operational TS/SCI environments covering Army Intelligence TS/SCI requirements.

As the Army extends cloud to CONUS and OCONUS locations, the cARMY common shared services will need to extend to these locations. This will move the Army towards having enterprise common shared services that can support the unified global network.

Tasks:

- Pilot extension of cARMY common services to CONUS and OCONUS private clouds including data centers and tactical, as well as the capability to function in both connected and disconnected states

- Expand services for SECRET Environments for research and scientific development (cARMY-XS)
- Expand pilot of extension of cARMY common services to all CONUS and OCONUS private clouds

Enterprise Cloud Service Provider Vehicles

Prior to the March 2021 establishment of the Army's first Enterprise CSP vehicle, the Army purchased Cloud Service Offerings (CSOs) inefficiently through hundreds of smaller contract vehicles, resulting in poor buying power. Due the nature of these contract vehicles, systems were often deployed in a "lift-and-shift" manner and failed to take advantage of commercial cloud benefits. Under the old contracts, the Army rarely owned the CSP accounts themselves, which reduced control over their own mission systems and data and made contract transitions from one service provider to the next difficult. The Army will continue to take the lessons learned from this Enterprise CSP vehicle to determine the appropriate path forward for future Enterprise CSP procurement mechanisms, including review and consideration of the DoD's Joint Warfighting Cloud Capability (JWCC).

Tasks:

- Continue to identify Army clouds that are not currently under the Army Enterprise CSP vehicle and are not consuming cARMY services
- Integrate disparate cloud accounts into the cARMY ecosystem and the Army Enterprise CSP vehicle
- Analyze future Enterprise CSP vehicle options to identify a solution that will provide the Army the best value and most efficient processes to execute the mission

3.2 SO 2: IMPLEMENT ZERO TRUST ARCHITECTURE

An important aspect of securely extending cARMY is implementing a ZTA in accordance with Executive Order 14028 and in alignment with the DoD Zero Trust Reference Architecture. As defined by Executive Order 14028, "The term 'Zero Trust Architecture' means a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries."[6] The Army will take advantage of a ZTA to incorporate a secure SD-WAN, granting the Army a global cloud network without routing all traffic to a boundary cloud access point and providing touchpoints to the DoDIN only where necessary.

LINES OF EFFORT

Zero Trust Transport

A key part of the ZTA are the transport mechanisms that allow the cloud to extend globally and securely. Implementing a ZTA allows the Army to utilize transport mechanisms such as SDN technologies that enable SD-WAN, commercial cloud global backbone, and commercial satellite communications (LEO, MEO, GEO), among others, while also enabling the delivery of services and data to the warfighters across all domains. SDN virtualizes the capability of physical transport devices such as routers and layer-3 switches to provide Local Area Networks (LANs) with highly available and scalable logical optical transport links. These logical circuits can dynamically route and offload traffic as needed to other logical circuits during peak operations. SDN can also be used to enable virtualized load-balancing between nodes deployed at facilities, such as datacenters, to make application data highly available. The secure access objects will be protected resources governed by the ZTA protection surface to include applications, services, APIs, operations, and data.

Tasks:

- Architect transport paths for the global cloud ecosystem from the enterprise to the tactical edge to include commercial cloud backbone and satellite communications
- Determine where SDN nodes, master control nodes, and Secure Access Secure Edge (SASE) solutions will be deployed and what routing and security policies will be defined
- Determine secure access enforcement points including the automation, orchestration, and micro-segmentation of applications
- Determine routing and security policies for access to IT services, CSP SaaS offerings, and Mission Partner data
- Enable connectivity and enforce policies for selected transport paths

[6] https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

Cloud-native Zero Trust Capabilities

Because the ZTA is comprised of several different solutions that provide ZT capabilities, the Army will determine what solutions to use to meet those capabilities. While some new solutions may need to be added, it is also possible that existing solutions can be modified to meet the desired capabilities.

Tasks:

- Determine the cloud-based security solutions that will contribute to the global cloud ZTA, including existing and new solutions
- Determine and implement changes to existing solutions to meet global cloud zero trust capabilities
- Implement new solutions to meet global cloud zero trust capabilities

Zero Trust Control

The ZTA relies on configuration policies to define how security will be enforced, with a heavy emphasis on security orchestration and automation to automatically enforce and modify policies. As such, creation and modification of these policies and automations need to be carefully controlled.

Tasks:

- Determine configuration management solution for the global cloud ZTA
- Establish a configuration and change control board to oversee the ZTA
- Determine the architecture for Security Orchestration and Automated Response (SOAR)
- Establish the automation playbooks that will be used by the ZTA

SO 3: ENABLE SECURE, RAPID SOFTWARE DEVELOPMENT

The Army needs to be able to field mission-critical applications in a rapid, secure manner, while taking advantage of cloud platforms to make the applications scalable and adaptable in order to reach the goals of the Army of 2030. To that end, the ECMA collaborated with

> **The Army needs to be able to field mission-critical applications in a rapid, secure manner, while taking advantage of cloud platforms to make the applications scalable and adaptable.**

the Army Futures Command (AFC) Software Factory to deploy the Code Resource and Transformation Environment (CReATE), a platform in cARMY that utilizes DevSecOps tools and continuous integration / continuous delivery (CI/CD) pipelines. In alignment with the DoD Software Modernization Strategy[7] published in February 2022, CReATE will expand to enable continuous risk management framework (cRMF) activities to accelerate authorized deployments of software. The standardization of CReATE's DevSecOps tools and cARMY's continued development of common shared services streamlines the accreditation process, reduces technical debt, and increases the Army's security posture. At the same time, an increasing amount of low/no code environments allows the Army to develop capabilities without extensive development background or experience. The CReATE DevSecOps Playbook provides Army developers with the National Institute of Standards and Technology (NIST) and industry best practices to guide agile, cloud-native, rapid software development within the compliance standards for tenancy in the cARMY environment.

LINES OF EFFORT

Expand CReATE

Expanding CReATE will help accelerate secure and rapidly developed applications and streamline the ATO process for applications. CReATE will be used as a baseline to incorporate similar DevSecOps capabilities within cARMY to support OCONUS and tactical environments where connectivity to CReATE may be intermittent or non-existent.

Tasks:

- Integrate deployment to a variety of container platforms, including Docker and Kubernetes, and to approved serverless technologies

[7] https://media.defense.gov/2022/Feb/03/2002932833/-1/-1/1/DEPARTMENT-OF-DEFENSE-SOFTWARE-MODERNIZATION-STRATEGY.PDF

- Expand CReATE to all cARMY environments—IL2-6 and all CSPs
- Incorporate CReATE into cloud and ZT operations to support infrastructure as code and automation playbooks
- Design and deploy DevSecOps platforms based on CReATE to deploy to OCONUS clouds

Deploy SaaS Low/No Code Development Environments

Low/no code environments and Robotic Process Automation (RPA) platforms enable the Army to rapidly develop capabilities with minimal development background, resulting in faster deployment of software as well as enabling users at all echelons to develop new apps and bots to meet their mission needs in a fully accredited environment. The Army will standardize on enterprise commercial IT Service Management and Customer Service Management tools as the initial low/no code platform, as well as an enterprise RPA Platform for business process automation.

Tasks:

- Finalize the Enterprise License Agreement (ELA) for the low/no code platform
- Configure and deploy the low/no code platform
- Pilot RPA infrastructure with identified Mission Area Partner
- Expand RPA pilot to be a shared service across the enterprise with infrastructure managed in cARMY and functional owners identified in each Mission Area

SO 4: ACCELERATE DATA-DRIVEN DECISIONS

In partnership with the Business Mission Area (BMA) and Office of Business Transformation (OBT), the ECMA successfully utilized the Army's Enterprise Data Services Catalog (EDSC) for all data entering cARMY to inform what data exists in Army cloud and how it can be accessed and utilized. Building on this work, the Army must maximize its ability to utilize its data in warfare to be equipped to battle in MDO and to outmatch peer and near-peer adversaries. This SO includes real-time and near real-time analytics of data, as well as taking full advantage of Artificial Intelligence/Machine Learning (AI/ML) for both defensive and offensive operations. Teaming with our Mission Partners, the Army will employ a cloud-based data management platform enabling the warfighter to gather, structure, analyze, discover, and consume data. These shared data management services and environments will allow for the processing, cataloging, discovery, and analytics of operational data for unstructured, semi-structured and structured data across the Army. The use of a hybrid-cloud architecture to include in-cloud and near-cloud processing, high performance computing, and tiered storage models to accommodate data availability and retention will accelerate the operationalization of data regardless of whether the current service brokering the data will be migrated or modernized to accommodate a cloud-based architecture.

LINES OF EFFORT

Enterprise Data and Analytics Services

The Army must establish a cloud-native Enterprise Data and Analytics Services providing new industry capabilities and support rapid, data-driven application development to provide data enabled decisions at echelon and meet the scale and speed needs of the Army. These services will enables all Mission Areas in the areas to leverage access to authoritative data through APIs and microservices, as well as serve as an integration platform for future system requirements such as Enterprise Business Systems – Convergence as well as the Army's future Vantage data platform requirements.

Tasks:

- Create a reference architecture for a cloud-native Enterprise Data & Analytics Services
- Deploy and integrate prioritized Enterprise Data & Analytics services in cARMY
- Onboard and ingest prioritized Enterprise data sources in coordination with Army Commands (ACOMs), Army Service Component Commands (ASCCs), Direct Reporting Units (DRUs), and the Army Data Board

Establish API Orchestration Engine

Delivering a centralized Enterprise Level Platform for the full lifecycle (design, development, deployment, monitoring, and retirement) of APIs continues to be a priority for the ECMA as it enhances the ability to develop microservices. Once instantiated, the API

Management Platform will provide a single point for Army API fronted capabilities, allowing for rapid recognition of capabilities in real time. Awareness of all capabilities, from simple Extract, Transform, Load (ETL) functions to accessing cARMY Data Warehouses, will promote data sharing and reduce burden on both legacy and future systems.

Tasks:

- Refine Concept of Operations
- Deploy Platform to Production
- Determine Chargeback Model
- Develop Onboarding Guidance for Program Managers & developers

SO 5: ENHANCE CLOUD OPERATIONS

Since the release of the Army Cloud Plan 2020, the ECMA established cloud environments in both AWS and Azure that are approved for use at IL2-6 and developed initial processes that enable the Army to take advantage of the cloud. The Army must continue to scale by automating and injecting customer transparency across the Cloud Modernization Approval Process (CMAP) to support all the strategic objectives in this strategy and the Army's modernization priorities. This includes educating the workforce on cloud, accelerating the modernization and migration of systems and applications to cARMY, and automating supporting processes and workflows to make them more efficient.

LINES OF EFFORT

Army Cloud Portal

The Army requires an enterprise cloud portal that integrates all cloud initiatives across the Army and our Mission Partners to include the DoD, industry, and academia. The Army Cloud Portal will connect current and future customers with the tools, training, and resources to enable self-service capabilities, resulting in the delivery of more effective solutions to the warfighter. Customers will also be able to use this portal to complete online training, access educational content, view the cARMY enterprise service catalog, and start their journey to cloud. The portal will promote community engagement through forums, where customers can engage with each other, and forms, where customers can submit requests to the ECMA.

"The Army must continue to scale by automating and injecting customer transparency across the Cloud Modernization Approval Process (CMAP) to support all the strategic objectives in this strategy and the Army's modernization priorities.

Tasks:

- Design, build and deploy the Cloud Portal
- Establish the cARMY Enterprise Service Catalog and reimbursable cost models
- Incorporate on-demand training to help inform customers about cloud and provide role-based trainings for cloud architects, platform engineers, software developers, and other team roles
- Develop whitepapers, frequently asked questions (FAQs), and videos for the Cloud Portal to communicate cARMY capabilities and processes to the Army
- Expand the Army Cloud Portal to support data sharing with Mission Partners

Cloud Service Management Platform

The ECMA will leverage a cloud-based service management platform to centralize customer service capabilities and automate workflows accelerating the CMAP from initial customer intake to operations and maintenance in a cARMY production environment. This will create a traceable and automated review process between the ECMA and their customers. The service management platform will integrate with Army data sources such as the Army Portfolio Management System (APMS), eMASS, and EDSC to generate data mappings, create cloud user roles, and validate security artifacts to automatically provision environment blueprints and develop common shared service mappings, resulting in enterprise-wide service automation and integration for cARMY.

As the Army becomes more cloud dependent, it is increasingly important for Army personnel to understand the cloud as a core competency.

Tasks:

- Develop the CMAP Planning workflow to include integration with the Army's Enterprise CSP Vehicle, CReATE and the Army's Cybersecurity Service Provider (CSSP), C5ISR
- Develop core IT Service Management modules
- Develop the CMAP onboarding workflow to include blueprint builds and common shared service mapping
- Automate customer case management and inquiry response via virtual agents

SO 6: ENABLING THE CLOUD WORKFORCE

As the Army becomes more cloud dependent, it is increasingly important for Army personnel to understand the cloud as a core competency. Users should understand how the devices and systems they use to support the Army mission interact with and can create potential attack vectors. Systems administrators, network operators, data engineers, and developers, among others, need to understand how to design and operate secure, scalable, and high performing systems and applications that maximize the use of the cloud. As such, it is important for the Army to establish a cloud career path as detailed in the Army Digital Human Capital Strategy.

LINES OF EFFORT

Army Cloud Career Path

The Army will establish an Army Cloud Career path to support the future of the cloud workforce. Efforts will focus on the steps that follow hiring talent and provide career pathing to the cloud workforce that identifies innovative, technology enabled ways to improve employee engagement, career path agency, and data-informed and talent-based decision making.

Tasks:

- Design the cloud workforce in accordance with the Army Digital Human Capital Strategy to establish a workforce framework, identify career stage assessment and modeling, define workforce constraints to enhance permeability, have subject matter experts within external guidance/alignment, and accelerate diversity, equity, and inclusion strategies
- Enhance career mobility and partnerships to prioritize workforce skills, inform external recruitment strategies, develop internal talent, and mature skills tracking
- Establish a culture of learning by building a learning risk framework, implementing a digital workforce network and virtual collaboration environment, establishing a culture framework, and democratizing data for large scale consumption
- Update the Army Training and Certificate Tracking System (ATCTS) to include terms, certificates, and training requirements. Cloud account registration will utilize Common Access Registration (CAR) with Role Based Access Control (RBAC) for account roles and permissions

Cloud Savvy Workforce

The Army will establish a training program to provide the workforce and leadership with foundational cloud knowledge. This will help members of the workforce who are not directly involved with cloud understand concepts and be better informed when making decisions such as those that involve modernizing applications for cloud.

Tasks:

- Identify learning pathways and modalities applied to Total Army
- Establish a digital literacy program to provide oversight and insight into the developmental experiences of the civilian digital workforce
- Identify and catalog available learning and development opportunities
- Incentivize and require Cloud Savvy certification

SO 7: PROVIDE CLOUD COST TRANSPARENCY AND ACCOUNTABILITY

Cloud's utility-like, variable cost structure can easily lead to underutilized services and unexpected, avoidable costs. To combat this, the Army will use a combination of enterprise provided common-services and cloud consumption tracking for all cloud consumers. This approach reduces customer burden for common services and facilitates user-level control for monitoring, forecasting, deploying, and optimizing cloud investments at all echelons. The Army has made great strides towards providing transparent cloud infrastructure costs for reporting and optimization. The Army deployed an Enterprise Cloud Tracking Software that provides access to near real-time data of cARMY service costs across commercial cloud environments. Critical next steps to achieving this SO are to expand this capability for all commercial cloud environments, continue the intake of Army cloud consumers in order to build cost accountability, facilitate data-driven investment decisions, and forecast with fidelity the Army's future cloud costs.

LINES OF EFFORT

Refine Funding Model for Cloud Services

The Army established a list of common services to be provided at no cost to all Army customers. These common services will mitigate duplication of commonly required cloud resources such as identity management and environment management. However, certain administrative, development, and data services in support of user workloads may require chargeback to accommodate variable licenses and infrastructure services. These variable costs must be accounted for in a customer's actual usage, to ensure the customer can appropriately forecast, program, and resource for these costs in the future. The ECMA will provide transparency based on actual services consumed and provide accurate forecasts to better inform the POM build, as well as capture the necessary data elements to report IT investments and communicate with Army financial systems.

Tasks:

- Maximize user adoption of commercial cloud in support of the Army's transition to cARMY environments
- Identify and catalog administrative, development, and data services to be monitored for reimbursable and centrally appropriated options
- Identify critical data elements for cloud resources to tie CSP resources to Army budgetary and financial identifiers, e.g., KEY5 and APE
- Develop analysis and reporting of infrastructure-as-a-service reporting by customer to assess cloud billing and forecasting aligned to CSPs, Technology Business Management (TBM), and Army financial structure

Enterprise Cloud Tracking Software

The Army Enterprise Cloud Tracking Software will provide cost transparency into cloud accounts under the Army Enterprise CSP vehicle. This tool reports utilization metrics and provides customer data transparency to drive investment decisions and reduce manual and inefficient administrative business processes. In addition, the tool presents optimization options to reduce overrun risk for cloud investments through cloud consumption analytics and alerts to caution application owners of funding issues. The Enterprise Cloud Tracking Software is the authoritative source for TBM reporting of cARMY CSOs.

Tasks:

- Populate the Enterprise Cloud Tracking Software with all Enterprise CSP vehicle accounts
- Integrate Enterprise Cloud Tracking Software with GFEBs to support internal accounting transaction and allow funding models flexibility
- Automate Enterprise Cloud Tracking Software with contract management to support automated contract management for cloud funding and execution

The Army must prioritize its financial and personnel resources to relentlessly and purposefully pursue the modernization efforts outlined in this cloud plan in order to maintain decision dominance against U.S. near-peer adversaries.

CONCLUSION

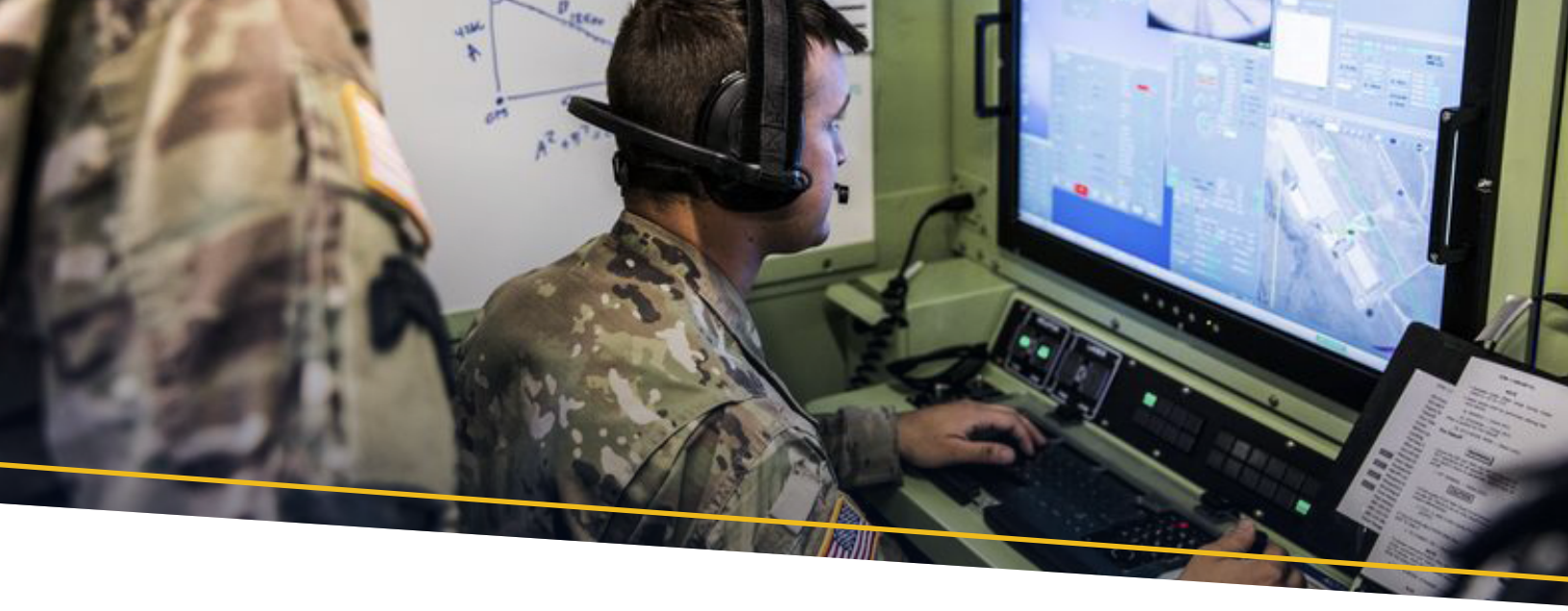
In a time when technology is advancing and adversary attacks using information technology are becoming more sophisticated, it is imperative for the Army to gain both defensive and offensive competitive advantage. The Army will achieve this advantage by converging its networks, including cloud, and using its data efficiently and effectively to inform multi-theater, multi-domain operations. The cloud is a key enabler of the Army's modernization goals and will allow the Army to use critical technologies to improve data-driven decision making for the warfighter. The Army must prioritize its financial and personnel resources to relentlessly and purposefully pursue the modernization efforts outlined in this cloud plan in order to maintain decision dominance against U.S. near-peer adversaries.

As the Army continues to gain experience and lessons learned through its data optimization and cloud modernization efforts, it should be expected that the Army Cloud Plan will be updated accordingly. This will be a living document maintained by the ECMA and modified with feedback from the community, leveraging the resources identified in the Army Cloud Roadmap.

METRICS

Metrics are an important aspect of the Army Cloud Plan 2022 as they will help determine the Army's effectiveness in achieving its strategic objectives. The metrics shown below are high-level, covering the entire Army Cloud Plan 2022. These metrics will inform various reporting requirements. Additionally, targeted metrics will be developed to capture and measure success for each strategic objective and the lines of effort. The Office of the Primary Responsibility (OPR) and Office of the Coordinating Responsibility (OCR) will be established for the strategic objectives as they are expanded.

- Percent reduction in Army data centers and data processing nodes
- Percent of total Army applications hosted in cARMY (commercial or AEPC)
- Average throughput time from initial customer intake to deployment in cARMY
- Ratio of annual spend in on-premise data centers to cloud
- Total costs avoided or saved using cARMY common services
- Uptime of cARMY shared services for CONUS and OCONUS
- Percent of cloud traffic leveraging commercial transport/SATCOM
- Percent of users leveraging BYOD/VDI for cloud access
- Percent time reduction to achieve ATO
- Percent of ZT capabilities based on DoD ZTRA deployed
- Mean time for vulnerability identified to application patched
- Percent of applications developed using DevSecOps or low/no code platforms
- Percent of data interfaces leveraging APIs
- Ratio of data storage in shared drives vs. cloud storage
- Percent of Army source data registered in EDSC
- Percent of Army Senior Leaders trained or certified, e.g., Cloud Digital Leader training
- Annual employee turnover rate of digital/ technical roles
- Percent of Army new hires using the new Cloud Career Path
- cARMY customer satisfaction, e.g. Net Promoter Score



GLOSSARY OF TERMS

TERM	DEFINITION
Army Enterprise Private Cloud (AEPC)	A collection of IT resources that will be hosted in select regional locations to provide computing resources through the following: • On-demand self-services: users can provision and manage resources • Broad network access: resources are generally accessible • Rapid elasticity: the ability for resources to scale in and out as needed • Resource pooling: resources are shared across applications • Measured service: resource utilization is tracked These resources would be wholly owned and operated by the Army organization that consumes the cloud services, without any sharing of infrastructure or co-location of resources used by an external organization.
cARMY	The Army's General Purpose cloud environment along with the necessary Cybersecurity Service Provider (CSSP) and the centrally-provided Common Shared Services in the environment. cARMY is the directed hosting environment for all Army cloud activities aligned to the Infrastructure and Platform as a Service design patterns.
cARMY Common Shared Services	A set of services that most tenants of a cloud environment will require to support their applications. Centrally consuming these services, instead of deploying the same set of services for each client, reduces overall costs and enables a more scalable cloud enterprise.
Enterprise Data Services Catalog (EDSC)	The Army's stand-alone data catalog that enables the creation of an Army Enterprise data source inventory (for both authoritative and nonauthoritative sources) by capturing and managing metadata describing the data sources and is the single point of reference for all Army data sources.

Impact Level (IL)	A combination of the sensitivity of the information stored and the potential impact of an event resulting in the loss of confidentiality, integrity, or availability of that information. An environment with a higher impact level supports more sensitive data: • **IL2 –** Accommodates information approved for public release • **IL4 –** Accommodates DoD CUI • **IL5 –** Accommodates DoD CUI and National Security Systems • **IL6 –** Accommodates DoD Classified Information up to SECRET
Infrastructure as a Service (IaaS)	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components, e.g., host firewalls.
Platform as a Service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
Secure Access Secure Edge (SASE)	A security framework prescribing conversions of security and network connectivity technologies into a single cloud-delivered platform to enable secure and fast cloud transformation.
Security Orchestration and Automated Response (SOAR)	A capability that enables threat and vulnerability management while automating incidents response. A SOAR also provides the ability to enforce ZT policies while orchestrating security actions. Although typically a single platform, SOAR activities can also be performed using cloud-native tools.
Software as a Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.


OFFICE OF THE
UNITED STATES ARMY
OCIO
CHIEF INFORMATION OFFICER