



# The Army Cloud Plan

2020

*“...The Army cannot maximize its **modernization strategy** without the cloud, which is the backbone for artificial intelligence.”*

**- HON Ryan D. McCarthy**

*United States Secretary of the Army*

Page Intentionally Left Blank

## Table of Contents

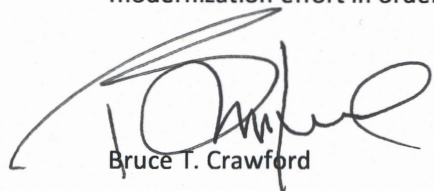
Executive Summary .....	4
The Mission Imperative .....	5
The Age of Disruption .....	5
Delivering Digital Overmatch.....	5
The Digital Landscape .....	6
Forces at Play.....	6
Strategic Objectives .....	6
Modernization Imperatives .....	7
Digital Transformation.....	8
Hybrid, Multi-Cloud Environment Principles .....	8
Adaptive Processes.....	9
Cloud Native Design .....	9
Plan of Attack .....	10
Centralized Cloud Management.....	10
Cloud Architecture.....	11
Common Shared Services .....	12
Data Discovery and Operationalization .....	12
Rationalization and Modernization .....	13
Early Adopters and Fast Followers .....	14
Tactical Cloud and Network Optimization.....	14
DevSecOps Services.....	15
Rapid Acquisition .....	15
Equipping the Workforce .....	16
Designed to Adapt.....	16
Conclusion .....	17
Appendix A: Army Enterprise Cloud Ecosystem Common Services List (IOC) .....	18
Appendix B: Army Enterprise Cloud Ecosystem Tiered Services Model.....	20
Appendix C: Army Title 10 Enterprise Cloud Ecosystem CONUS Common Operating Picture ....	21

# Executive Summary



As recognized in the 2018 National Defense Strategy (NDS), cyberspace is now a war-fighting domain. In order to compete and win in this domain, the total Army must leverage modern information technology (IT) and methodologies to transform itself into an agile, lean, software-enabled Service that can respond to adversaries on the digital battlefield at the speed of war. The Army Cloud Plan communicates the Army's vision for leveraging the cloud to maintain information superiority and to deliver digital overmatch. Total Army Digital Overmatch is the Army's ability to be stronger, better-armed, and more skillful than its adversaries in the use of information technology. The Army Cloud Plan provides a strategic approach to the changing digital landscape and supports the Army Data Plan (ADP) to enable a globally accessible, standards-based environment where data and information are visible, accessible, understandable, trusted, interoperable, and secure (VAUTIS) throughout its lifecycle. The ability for the Army to quickly create, discover, and leverage its own data is paramount in upholding the oath to protect the United States from all enemies foreign and domestic. Therefore, the Army must adapt its processes to be more agile, its network and hybrid cloud environments (to include strategic data center footprints) to be more elastic, IT software design and fielding approaches to be more resilient to physical failures, and organizational structures and training to be more effective at information warfare.

The Army Cloud Plan lays out the following six strategic objectives: Accelerate Data Driven Decisions, Decrease Time to Field Software, Optimize the Security Accreditation Process, Establish Cloud Design, Software Development and Data Engineering as a Core Competency, Design Software to Adapt to an Unpredictable World, and Provide IT Asset/Cost Transparency and Accountability. The plan then describes the modernization imperatives, digital transformation elements and the Plan of Attack the Army must use to achieve these six objectives and begin its journey to the cloud. The Army's ability to master cloud computing and its use is a critical enabler to the pursuit of leveraging Artificial Intelligence (AI) and Machine Learning (ML) in cyberspace warfare. The Army must relentlessly and purposefully pursue this modernization effort in order to maintain digital overmatch against U.S. near-peer adversaries



Bruce T. Crawford

Lieutenant General, U.S. Army

Chief Information Officer/G-6



Paul B. Puckett III

SES

Director, ECMO

*“You have no choice but to operate in a world shaped by globalization and the information revolution. There are two options: **adapt or die.**”*

*- Andrew Grove, Former CEO, Intel Corporation*

# The Mission Imperative

## The Age of Disruption

Today, the world is operating in an Information Age of disruption where access to real-time information to enable data-driven decisions is the new standard to compete and win. This digital innovation movement has extended to the battlefield where U.S. adversaries are actively increasing their digital warfare capabilities, utilizing data as a strategic asset, and leveraging the cloud as an enabler to expedite and scale the impacts of that data below the level of armed conflict. In contested areas today, Soldiers are immediately met with cyber offensive operations to disrupt or dismantle lines of communication, limit access to and the integrity of information, and degrade the Army’s ability to make accurate decisions at the speed of war. The rise of machine learning (ML) and artificial intelligence (AI) will soon give way to global weaponized AI, and the hand that wields it will define the future of the world. As recognized in the 2018 National Defense Strategy (NDS), cyberspace is now a war-fighting domain.<sup>1</sup> In order to compete and win in this domain, the total Army must leverage modern information technology (IT) and methodologies to transform itself into an agile, lean, software-enabled Service that can respond to adversaries on the digital battlefield at the speed of war.

## Delivering Digital Overmatch

This Army Cloud Plan communicates the Army’s vision for leveraging the cloud to maintain information superiority and to deliver digital overmatch. **Total Army Digital Overmatch is the Army’s ability to be stronger, better-armed, and more skillful than its adversaries in the use of information technology.** In order to achieve and sustain this new imperative, the Total Army’s ability to recruit, equip, train, retain and grow the warfighter will require Army schoolhouses, doctrine, acquisition, organization and leadership to be optimized to fight and win wars in the digital realm.

This Army Cloud Plan supports the 2019 Army Modernization Strategy “in the rapid and continuous integration of all domains of warfare – land, sea, air, space, and cyberspace – to deter and prevail as we compete short of conflict, and fight and win if deterrence fails.”<sup>2</sup>

This Army Cloud Plan supersedes the Army’s 2015 Cloud Strategy and will be updated as feedback drives the need for refinement and clarity.

---

<sup>1</sup> Summary of the 2018 National Defense Strategy of The United States of America, Secretary of Defense, 2018

<sup>2</sup> Army Modernization Strategy: Investing in the Future. 2019

# The Digital Landscape

## Forces at Play

This Army Cloud Plan provides a strategic approach to the changing digital landscape and supports the Army Data Plan (ADP) to enable a globally accessible, standards-based environment where data and information are visible, accessible, understandable, trusted, interoperable, and secure (VAUTIS) throughout its lifecycle.<sup>3</sup> The ability for the Army to quickly create, discover, and leverage its own data is paramount in upholding the oath to protect the United States from all enemies foreign and domestic.

**Therefore, 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 organizational structures and training to be more effective at information warfare.**

## Strategic Objectives

The Army's desired Strategic Objectives (SOs) of the 2020 Army Cloud Plan are as follows:

1. **Accelerate Data Driven Decisions:** Provide real-time and near real-time discovery, processing, analysis, and exploitation of service enabled Army data to support Joint All Domain Command and Control (JADC2) from the battlefield to the enterprise and back.
2. **Decrease Time to Field Software:** Enable continuous integration/continuous delivery (CI/CD) of software using a Development, Security and Operations (DevSecOps) methodology to automate processes, prioritize user feedback, employ cloud native technology, and converge cultures.
3. **Optimize the Security Accreditation Process:** Integrate security into the development, testing, certification and operational ecosystem to provide real-time verification, validation and remediation of the Army's security posture through automated security scanning, continuous monitoring and accredited software delivery pipelines and platforms.
4. **Establish Cloud Design, Software Development and Data Engineering as a Core Competency:** Posture the Army to transform its Soldiers, Civilians, organizations, and leadership and attract talent as industry experts in cloud infrastructure, software delivery and data engineering.
5. **Design Software to Adapt to an Unpredictable World:** Enable the creation of modern software solutions that lay a digital foundation capable of scaling with the growing quantity of real-time information.
6. **Provide IT Asset/Cost Transparency and Accountability:** Use of cloud will enable transparency and accountability for IT assets and their costs, through automated monitoring tools and dashboards ensuring efficient use of resources, and compliance with Federal and Department of Defense (DoD) directives and inquiries into IT spending.

---

<sup>3</sup> The United States Army Data Plan, November 2019

## Modernization Imperatives

In order to achieve the objectives identified in the previous section, and to operationalize the Army Cloud Plan, the following imperatives are required:

**Adjust Acquisition Strategies** - If software is to be created at the speed of operations, the acquisition strategy must adapt as well. Therefore, all new acquisitions must use cloud-smart principles, common shared services and Agile software development methodologies (e.g. lean startup, design thinking, DevSecOps) to support rapid delivery of standardized, reliable, integrated and secure mission capabilities. Leveraging Army-provided DevSecOps ecosystems, all new acquisitions should demand a service enabled architecture with automation of those tasks and processes that do not require human input across infrastructure, configuration, software, and testing. The Army also must tailor and streamline its pre-acquisition approval and governance processes to accelerate IT investment decisions. As the Army identifies data and services for modernization to a cloud native architecture, rapid acquisition approaches may be required to reduce the risk of costly and inefficient modifications to existing contracts incapable of adapting to a cloud native environment.

**Develop and Execute a Cloud Talent Management Plan** - Developing and executing a talent management plan is essential to address the Army's need for multi-disciplinary teams of cloud and data professionals to ensure data is VAUTIS throughout its lifecycle, for all authorized users. The U.S. Office of Personnel Management (OPM) recognized the rapidly changing field for data science with several occupational series for civilian positions. Overlapping skills involving data analysis, analytical applications, big data engineering, algorithms, domain expertise, statistics, and ML were identified in one or more domains. The Army must establish the means to enable all Civilians and Uniformed Personnel to pursue a role in Digital Innovation that supports their career growth and branch of service to ensure that digital overmatch is not isolated to the career of the Signal Corps. Implementation of a talent management plan that supports the Army Cloud Plan will enable those closest to the needs and challenges to impact those fields with software development, data science, or relevant digital innovation specialties. Data, software and cloud design education is necessary to ensure the existing workforce is appropriately equipped to enact the necessary paradigm shift in Army support and management activities to assure a mission-ready workforce.

**Establish Governance** - Establishing a governance structure for Army data and cloud management is a foundational element to sustainable digital overmatch. The structure includes dedicated management roles and responsibilities as well as advisory and decision-making bodies where identified architectural or data governance issues must be resolved. Much like site reliability engineering, governance bodies should look to identify means to eliminate their need for manual oversight and create solutions that address not only point-in-time decisions but eliminate repeated issues of the same form. The Enterprise Cloud Management Office (ECMO) will establish onboarding processes, monitor service usage and adherence to architectural standards. The Enterprise Cloud Working Group, led by the ECMO, will be the official means to communicate lessons learned and challenges experienced adopting cloud technology that in turn drive the creation or modification of standing policies impacting the Army's cloud modernization effort across the enterprise. To enable the scale and communication of cloud governance, each Army Command (ACOM), Army Service Component Command (ASCC), Headquarters Department of the Army (HQDA) Staff Office, and Direct Reporting Unit (DRU) will establish expertise in cloud architecture,

data engineering, and software development, with the long-term goal of operating self-sufficiently in the cloud.

**Build a Secure Cloud Architecture** - A well-defined and well-constructed cloud-based architecture is a critical mission enabler. The architecture must use a Cloud-Smart, Data-Smart approach as identified in the 2018 DoD Cloud Strategy. The architecture will focus on enabling mission criticality, data integrity, operational resilience and availability in a secure environment. With the goal of reducing technical debt of long-term sustainment mission capabilities and duplication of effort, the Army will deliver centrally resourced and available Common Shared Services, Data Management Services, and Software Development Services globally to apply cloud-native design principles. The Army hybrid-cloud architecture will also incentivize teams to build to the highest abstraction of cloud services to leverage Software as a Service (SaaS) and Platform as a Service (PaaS) offerings over Infrastructure as a Service (IaaS) where possible to reduce the overhead of technical debt accrued over time.

**Develop and Enforce Data Standards and Service Interfaces** - Data standards articulate data formats, metadata and documentation for data exchanges; however, constrained system integration often takes the form of point-to-point interfaces. In order to create interoperable, accessible and visible services, all new services deployed to a cloud architecture will have clearly defined interfaces and well-documented interface specifications to include the schemas and methods for how data is structured and exchanged. Legacy systems required for transitional services moving to an open and scalable cloud architecture will require open service brokers to be created on their behalf such as the OpenAPI specification. Data standard and interface specifications will be adjudicated by the Army Data Board (ADB) and the mission area data officers (MADOs) working directly with the ACOMs, ASCCs and DRUs.

**Provide and Ensure Data Protection** - An evolution in Army data protection is needed in order to facilitate digital overmatch. The Army requires modern security paradigms, controls, and frameworks in order to ensure that all data produced and consumed is VAUTIS. Data tagging, centralized authentication and authorization and encryption of data at rest, in transit, and in use as well as secure methodologies for key management must be leveraged to ensure a zero-trust model. Zero-trust is a security model based on the principle of maintaining strict access controls and not trusting anyone or any system by default, even those already inside the network perimeter. The use of Application Programming Interface (API) management and policy enforcement will ensure that data access is assured at the point of consumption. The Army will enforce zero-trust principles when moving into a cloud-based environment.

# Digital Transformation

## Hybrid, Multi-Cloud Environment Principles

The Army will deliver an ecosystem of integrated, hybrid cloud environments with parity of online, on demand shared common services, modern data management, software development, testing and fielding technologies. Although the end-state will be a hybrid cloud environment, the Army will focus its effort on leveraging commercial and off-premises cloud solutions. This environment will span all classifi-



cation fabrics and enable the consolidation of the Army's current disparate cloud environments to reduce the duplication of effort, reduce the security threat vectors to Army cloud-based systems, reduce the total cost of ownership, increase efficiencies, increase visibility and accessibility of Army data, and dramatically increase awareness and oversight of the unified Army cloud modernization effort.

The Army's cloud footprint will consist of a Continental United States (CONUS) based general-purpose hybrid-cloud environment across the Unclassified, Secret, Top Secret, Intelligence Community (IC) and Mission Partner environments. Commercial cloud services will be the preferred hosting location for CONUS based Army services to utilize compute and storage economies of scale. The Army will leverage a hybrid of DoD Enterprise Cloud Environments and Army fit-for-purpose cloud services that increase mission outcomes and reduce acquisition complexity. The Army will leverage a hybrid of both Commercial Cloud Service provided SaaS, PaaS, and IaaS capabilities and Army Enterprise Data Centers (AEDCs) to address the needs of Army IT systems, streamline development and testing, and provide information sharing within them. The Army will extend the CONUS based hybrid-cloud to strategic Regional Cloud Footprints into Outside the Continental United States (OCONUS) DoD approved environments. These will be strategically aligned with Army Regional Hub Nodes allowing for direct integration with the Army's Tactical Cloud and Edge Cloud environments to bring the global spectrum of needs of the Army to bear.

## Adaptive Processes

The Army will start small, learn, adapt, change, and grow in true agile fashion with respect to its use of the cloud. The Army will invest in early adopters and fast followers to leverage cloud computing in order to build on the readiness and lethality of the warfighter, learn quickly, adjust rapidly based on continuous feedback and scale the outcomes to the Total Army. To reduce the risk of technical debt incurred in this fast-paced adaptive process, the scale and rate of change must be managed strategically across the Army. Therefore, modernization efforts will follow both a strategic and tactical prioritization to address long-term and near-term needs. Over time, the Army will fundamentally transform itself with new tools, methodologies, organizational structures, leadership, and experiences to remain the dominant force in the digital realm. To enable the continuous improvement and transformation of the Army to endure into the future, these capabilities must be grown and refined within the Army.

## Cloud Native Design

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."<sup>4</sup>

Cloud Native Design will reduce the overhead of maintaining IT technology stack components and focus attention on the mission-enabling application and data layers while increasing security and resiliency of

---

<sup>4</sup> <https://github.com/cncf/toc/blob/master/DEFINITION.md>

Army applications. The use of CI/CD tooling for automation and centralized change and configuration management to secure the software supply chain of the Army's cloud native adoption is a foundational technology to manage the scale and complexity of hybrid-cloud architectures. The Army will prioritize the use of SaaS and PaaS (to include container technology) over IaaS models to reduce toil and overhead of maintaining IT systems. This will allow the Army to focus on software innovation and design versus maintenance. All systems providing a service consumed either internally to that system or externally to other systems should expose their data and functionality through version-controlled APIs, ascribing to the Open API standard where possible and registered in an Army code repository. Legacy systems undergoing modifications to adapt to a service-enabled architecture should design anti-corruption layers to support the transitional period.

# Plan of Attack

## Centralized Cloud Management

As described in the Institute for Defense Analysis (IDA) 2019 Report "On Developing a U.S. Army Enterprise Cloud Strategy", a centralized Army cloud office should have the following responsibilities.<sup>5</sup>

- Visibility into All Army Software and Data
- An Arbiter of Business Cases
- Keeping Cybersecurity in Check
- Managing Talent
- Modernizing Software Development Practices

In light of this study, the Secretary of the Army directed the establishment of the ECMO to be the central point for all efforts and processes related to cloud adoption across the Army. Initial Operating Capability (IOC) occurred in November 2019, with Full Operational Capability (FOC) expected in Q1FY21. FOC is defined as a fully resourced ECMO with cloud modernization subject matter expertise, established processes and procedures for adopting cloud computing, common services, operationalizing data and eliminating technical debt. To facilitate the centralized oversight and management of cloud adoption and support SO6, the ECMO, working with Program Executive Office Enterprise Information Systems (PEO EIS), Army Cyber Command (ARCYBER), HQDA G8 and Chief Information Office (CIO)/G6 Policy and Resources (P&R), will establish a hybrid-cloud account and finance management solution. Cloud account management in any HQDA-sponsored environments will mirror the organizational structure of the Army to allow decentralized execution of resources to support cloud adoption across each ACOM, ASCC and DRU with centralized management and oversight of those accounts provided by the ECMO. The ECMO will leverage machine learning to drive greater efficiency in the consumption of cloud services across the Army and gain transparency on the total cost of ownership of IT solutions fielded to the cloud. The ECMO will also establish a Cloud Solutions Onboarding Team and standardized application modernization process.

---

<sup>5</sup> On Developing a U.S. Army Enterprise Cloud Strategy, Institute for Defense Analyses; M. Marwick, N. K. Patel, Sept 2019.

In order to accelerate Army Cloud adoption, the ECMO, in coordination with Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASA[ALT]), will provide enterprise-level contracts for commercial Cloud Service Provider (CSP) offerings, common services, and application migration support. Where feasible and cost effective, the ECMO will leverage DoD Enterprise contracts such as the Joint Enterprise Defense Infrastructure (JEDI) contract, while establishing Army Enterprise Cloud Contracts based on mission requirements. In order to ensure there is sufficient visibility into cloud costs for decision-making, all systems/applications must comply with standardized contracting language, work breakdown structures, and data collection requirements in accordance with the HQDA EXORD 009-20 ADP Implementation in Support of Cloud Migrations.

#### Milestones and Measures:

- FOC of ECMO: Fully resourced with cloud modernization subject matter expertise, established processes and procedures for adopting cloud computing, common services, operationalizing data and eliminating technical debt (Office of Primary Responsibility [OPR]: CIO/ECMO, Targeted Completion Date (TCD): Q1FY21)
- Centralized Cloud Oversight and Management: Establishment of Cloud Account Management Tool (OPR: ECMO, TCD: Q4FY20), All existing Army cloud accounts captured and visible within tool (OPR: ECMO, TCD: Q2FY21)
- Enterprise CSP Contract established: CSP contract available for use in two CSPs (OPR: ECMO, TCD: Q4FY20)
- Enterprise Common Services/Managed Service Provider (MSP) Contract Established: Common Services/MSP contract in place for two CSPs (OPR: ECMO, TCD: Q2FY21)
- Enterprise Modernization Contract Established: Modernization contract available to application owners (OPR: ECMO, TCD: Q4FY21)

## Cloud Architecture

The ECMO will establish a standardized cloud architecture which is intended for use by all Army mission areas that fall under United States Code (U.S.C.) Title 10 control, and will support the 2018 DoD Cloud Strategy which states “the Department must address the unique mission requirements through a multi-cloud, multi-vendor strategy that incorporates a General Purpose cloud and Fit-For-Purpose clouds.”<sup>6</sup> The cloud architecture will support SO1 and be initially established at the unclassified level (Impact Level [IL] 2/4/5), followed by classified environments (for example, Secret/IL6, Top Secret/Sensitive Compartmented Information [SCI]). The environment will consist of general-purpose cloud (cARMY) as well as fit-for-purpose clouds for various Software as a Service (for example, Defense Enterprise Office Solution) and Infrastructure as a Service (for example, milCloud 2.0) offerings. Multiple Cloud Service Providers (CSPs) will be utilized as mission objectives require. Automation will be heavily utilized throughout the architecture to include employing concepts such as Infrastructure as Code (IaC), Configuration as Code (CaC), Software Defined Networking (SDN) and autoscaling. Several common cloud components will be established for use by tenants. The use of common cloud components is intended to accelerate the operationalization of data, security accreditation, software development, and cloud adoption. cARMY is currently authorized at IL 2,4,5 to provide common services in one CSP and will be authorized in a second CSP at IL 2,4,5 by 4QFY20. cARMY will be authorized at IL 6 in early FY21.

---

<sup>6</sup> DoD Cloud Strategy, Dec. 2018

Applications and Systems that fall under U.S.C. Title 50 control (i.e., Military Intelligence Program [MIP], National Intelligence Program [NIP]) will use the Army MI Commercial Cloud Service Provider (AC2SP) environment, authorized by Army G2. AC2SP is currently available at Top Secret and will have Unclassified and Secret environments available by the end of FY20.

#### Milestones and Measures:

- Cloud Architecture for Title 10 domain documented and established: Secure enterprise cloud environments architected, documented and available for Unclassified data (OPR: ECMO, TCD: Q4FY20), Secure enterprise cloud environments architected, documented and available for Secret data (OPR: ECMO, TCD: Q1FY21)
- Cloud Architecture for Title 50 domain documented and established: Secure enterprise cloud environments architected, documented and available for Unclassified, Secret, and Top-Secret data (OPR: G2, TCD: Q4FY20)

## Common Shared Services

A global Army Cloud environment must be secure, trusted, agile and resilient. In support of SO2 and SO3, and as a best practice for reducing complexity, increasing security, eliminating duplication of effort, and adopting cloud computing for the modernization of large organizations, the ECMO has applied lessons learned from early cloud adopters across the Army and fielded accredited and operational Common Shared Services for Impact Levels 2, 4 and 5 in what is known as cARMY. The ECMO will extend these services into additional CSP regions and classifications in addition to Enabling Services as customer priority dictates. With support from PEO EIS and ARCYBER, the Army will collapse all existing general-purpose cloud footprints into cARMY except AC2SP, which will continue to provide common services for the Title 50 domain. The Army may also support common services in a limited number of fit-for-purpose environments, such as milCloud 2.0. Cloud access and infrastructure will be brokered by automated, on-demand, self-service, templated designs and services. The environments will be accredited and managed for the Army with virtual infrastructure configuration management to focus resources on application and data challenges. As efficiencies are gained and environments are optimized, cARMY will be the enduring cloud footprint of the Army for all general-purpose needs and will extend these lessons learned applying common services into on-premise data centers both CONUS and OCONUS as Army Data Center Optimization is realized. The initial list of common services can be found in Appendix A.

#### Milestones and Measures:

- Cloud Common Services for Title 10 domain established: Cloud common services authorized for Unclassified data in two CSPs (OPR: ECMO, TCD: Q4FY20), Cloud common services authorized for Secret data in one CSP (OPR: ECMO, TCD: Q1FY21)
- Cloud Common Services for Title 50 domain established: Cloud common services authorized for Unclassified, Secret and Top-Secret data in one CSP (OPR: G2, TCD: Q4FY20)
- Reduce Cloud Footprints: all existing general-purpose cloud footprints collapsed into cARMY (OPR: ECMO, TCD: Q4FY22)

## Data Discovery and Operationalization

In FY20 and FY21, in support of SO1, the ECMO in coordination with the Chief Data Officer (CDO), the ADB, the G2, the Office of Business Transformation (OBT), and ARCYBER will establish data governance

and enablement within an Enterprise Data Services Catalog (EDSC), Enterprise Mission Services Portal, Enterprise Data Lake and Warehouse, and Enterprise Data Analytics Environment within cARMY and all future general use cloud environments. 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. A data architecture will be continuously refined by the ADB in tight coordination with the ACOMs, ASCCs, and DRUs as the Enterprise Data Lake and Warehouse are populated. 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 whether the current service brokering the data will be migrated or modernized to accommodate a cloud-based architecture in support of HQDA Executive Order (EXORD) 009-20.

#### Milestones and Measures:

- EDSC established: EDSC authorized for use in cARMY (OPR: CDO/ECMO, TCD: Q1FY21)
- Enterprise Mission Services Portal established: Enterprise Mission Services portal authorized for use in cARMY (OPR: CDO/ECMO, TCD: Q2FY21)
- Enterprise Data Lake and Warehouse established: Enterprise data lake and warehouse authorized for use in cARMY (OPR: CDO/ECMO, TCD: Q2FY21)
- Enterprise Data Analytics environment established: Enterprise data analytics environment authorized for use in cARMY (OPR: CDO/ECMO, TCD: Q2FY21)

## Rationalization and Modernization

Development and execution of the HQDA EXORD 009-20 ADP Implementation in Support of Cloud Migrations was a critical first step for the Army to see itself and to take account of mission area applications and the data they broker. The EXORD requires each mission area owner to inventory, rationalize, prioritize, and plan the disposition of the applications and data within their portfolio.

Once mission areas have identified their prioritized systems and data, in support of SO1, each ACOM, ASCC, HQDA Staff Office, and DRU will work with the ADB and Mission Area owners to conduct system and process analysis to gain efficiencies and operationalize data leveraging cloud computing. The assessment criteria will include the current customer value of the system, system architecture and security, authoritative data consumed or generated within the system, system dependencies in upstream and downstream workflows, the current availability and accessibility of the data, and contract viability for a cloud environment. This assessment should leverage all resources to include subject matter expertise, tooling to monitor access metrics and system resource utilization, continuous customer engagement for feedback, architecture assessment, business process mapping and modeling, contract rationalization, and mission area objectives to gain efficiencies and operationalize data. Beyond centralized migration support provided by the ECMO, command's self-migration to Army Enterprise Cloud Environments will be instrumental to the Army's movement to a cloud-native architecture. In addition to providing common services and lessons learned, the ECMO will consolidate cost data and self-migration plans across the Army's application to build a centralized view of the Army's migration progress. Impacts to the data and systems architecture contained in portfolio rationalization and modernization will be brought before the ADB through the MADOs in direct coordination with the owning ACOMs, ASCCs, HQDA Staff Office and DRUs for awareness, deconfliction, or prioritization.

#### Milestones and Measures:

- Systems/Applications/Data Prioritized: All mission area applications/systems and data rationalized and prioritized (OPR: Mission Areas, TCD: Q1FY21)
- Application Assessments Conducted: Initial set (top 50) of high priority data and their associated applications assessed for cloud readiness (OPR: ECMO, TCD: Q4FY21)

## Early Adopters and Fast Followers

In support of SO1, SO2 and SO3, the Army will employ an implementation methodology that will utilize a small set of early adopters of cloud-based technologies and design principles to ensure that the Army is effective in delivering outcomes for their respective mission area (MA) and that lessons learned will enable Army scale of adoption. Early adoption will be encouraged based on ADB prioritization of the effort. The use of data-driven metrics will allow for any course corrections in methodology and for cloud modernization playbooks to be created, shared and modified accordingly, providing flexibility and extensibility as edge cases are identified. Metrics will be tracked for both the mission area effectiveness and the process of delivering IT systems to a cloud environment. Mission area modernization efforts will employ the use of Objectives and Key Results (OKRs) and Key Performance Indicators (KPIs) derived by the customer, system owner, data owner, and mission area owner of the data or service being delivered to ensure the efficiencies the Army wants to gain or the availability and discovery of data is realized.

To optimize the onboarding process, in FY20 the ECMO will establish a Cloud Solutions office as the central broker of cloud subject matter expertise and process organization. By the end of FY20, an online, self-service portal will be created to systematize and standardize the Tactics, Techniques and Procedures (TTPs) and Standard Operating Procedures (SOPs) needed for each stage of cloud adoption. As this modernization effort grows in maturity and scale, the Army will focus on enabling the community responsible for delivering cloud enabled outcomes to support and collaborate with one another in their efforts. The Army's ability to deliver transformational change at Army scale requires early adopters and fast followers to work together and build knowledge together as the mission requires.

#### Milestones and Measures:

- Modernization Process Established: Develop, document, and test an end-to-end modernization process for Army applications (OPR: ECMO, TCD: Q4FY20)

## Tactical Cloud and Network Optimization

While cARMY will deliver CONUS based enablement and modernization for the Army, the Army must transform its Tactical and Edge cloud computing maturity and the networks that extend the Enterprise to the foxhole. OCONUS, Tactical and Edge cloud environments will be enabled with the expansion of CSP offerings and on-premises hybrid cloud IaaS and PaaS solutions to capitalize on existing hardware and software footprints across the Army, overseen by the Warfighting Mission Area. In support of SO1, Army Futures Command (AFC), in coordination with Program Executive Office Command Control Communications-Tactical (PEO C3T) and Army Forces Command (FORSCOM), will collaborate to deliver integrated tactical cloud solutions that extend the resources of the enterprise while accommodating for Delayed or Disconnected, Intermittently-Connected, Low-Bandwidth (DIL)-constrained environments.

The Army's efforts to optimize its enterprise and tactical systems to enable more open and integrated services and data will allow the Army to collapse its complex and isolated network architecture. These efforts will leverage a zero-trust model to ensure that any system integration and data access is secure, trusted, and authorized. This work will enable the strategic optimization of the networks connecting Army customers globally and reduce the complexity and often conflicting networking configurations across the Army's Department of Defense Information Network (DoDIN). Collapsing the network architecture will enable the simplification of the network security stacks and increase the Army's ability to visualize and improve prediction of network utilization over time, increasing availability, security and resiliency across its networks.

Milestones and Measures:

- Tactical Cloud Solution Architected and Implemented: Design and develop a tactical cloud solution (OPR: AFC, TCD: Q4FY22)
- Optimize the Network: Ensure data security while reducing the number of hops (and associated latency) data must traverse between the DoDIN and the commercial cloud (OPR: CIO/ECMO, TCD: Q4FY22)

## DevSecOps Services

The Army's ability to compete and win with software and data can be directly attributed to its ability to converge the communities of Development, Security, and Operations into an integrated team of teams capable of fielding mission relevant and secure software at the speed of need. In support of SO2, SO3 and SO5, and to accelerate collaboration across the Army, key technologies, such as CI/CD tools, Source Code Repositories, Static and Dynamic Analysis Security Test resources, Quality Assurance and Quality Control tooling, various PaaS and Container Orchestration services and project and product management resources will be provided by the ECMO, in coordination with the CDO, ASA(ALT), the Mission Areas, and AFC, beginning in FY20, with IOC planned for early FY21. Additionally, DevSecOps will enable the creation of security guardrails and accredited software development processes to accelerate the Authority to Operate (ATO) within the Army and streamline the maturation of rapid prototyping into operational capability for the warfighter. Through the standardization of DevSecOps tools and development of common services, these environments will streamline the accreditation process, reduce technical debt, and increase the Army's security posture.

Milestones and Measures:

- Initial CI/CD Pipeline Established: CI/CD pipeline authorized for use in cARMY (OPR: ECMO, TCD: Q1FY21)

## Rapid Acquisition

By the end of FY20, in support of SO2, the ECMO, working with ASA(ALT), will create clear policy and guidance to ensure Agile or Lean methodologies, test driven development, paired programming, and other software best practices are employed for new acquisitions. The policy and guidance will also ensure that all new software development embraces cloud native design patterns and consumes Common Shared Services within an ECMO approved environment within the Army Enterprise Cloud Ecosystem. As modernization efforts increase across the Army, access to various contract vehicles such as IT Engi-

neering and Services (ITES)-3S must increase to support requirements for cloud architects, data engineers, and software developers. Working with their respective ACOM, ASCC, HQDA Staff Office and DRU, each PEO will publish any available cloud-smart Basic Ordering Agreement (BOA) or Indefinite Delivery/Indefinite Quantity (IDIQ) capable of supporting these cloud modernization efforts. Additionally, the acquisition community will pursue use of contracting methods such as Other Transactional Authority (OTA) and recently updated DoDI 5000 series software acquisition pathways, as appropriate, to augment any lack of resources capable of supporting mission area modernization efforts across the Army.

Milestones and Measures:

- Standardized Cloud/Data Contract Language Established: Cloud and Data Contract Policy and Performance Work Statement (PWS) language developed and approved by ASA (ALT) (OPR: ASA(ALT)/ECMO, TCD: Q4FY20)

## Equipping the Workforce

In support of SO4 and to increase the IT competency across the entire Army, the Army will need to implement policies to attract, train,<sup>7</sup> and retain a workforce with the skills necessary to meet digital overmatch mission requirements. Beginning in FY20, in addition to providing industry-based training to re-skill and up-skill the workforce with cloud-based technologies and methodologies, the Talent Management Task Force, G-1, Training Program Evaluation Group, and Training and Doctrine Command (TRADOC) will pursue the establishment of the Digital Innovation Initiative for civilian and uniformed personnel. The Digital Innovation Initiative will include career focuses in modern software development, data science, design thinking, lean startup methodologies, business process mapping, product management, and all necessary modifications to enable career growth in digital innovation across any Army branch and civilian career program. The Digital Innovation Initiative will pursue the creation of Additional Skill Identifiers, Functional Areas, Military Occupational Specialties, Branches and Branch Specialties as needed to enable the Total Army to see career growth participating in digital innovation needs across the Army. The Digital Innovation Initiative will partner with AFC to pilot Software Factories across the Army comprised of uniformed and civilian personnel responsible for the design, creation, fielding, and iteration of data and software solutions to enhance the readiness and lethality of the Army.

Milestones and Measures:

- Cloud Training Available: Make commercial cloud training available to the entire Army (OPR: G1, TCD: Q4FY20)
- Digital Innovation Career Paths Established: focus recruiting and retention efforts on digital innovation career paths (OPR: G1, TCD: Q2FY21)

## Designed to Adapt

As the Army gains experience and lessons learned in 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

---

<sup>7</sup> On Developing a U.S. Army Enterprise Cloud Strategy, Institute for Defense Analyses; M. Marwick, N. K. Patel, Sept 2019.



document maintained by the ECMO and modified with constant feedback from the community executing the principles and leveraging the resources identified within it.

## Conclusion

Today, every domain is contested—air, land, sea, space, and cyberspace.<sup>8</sup> To gain the competitive advantage needed to win on the battlefield in the Information Age, the Army must operationalize its data and invest in resilient information ecosystems designed to provide and protect critical information for the Joint Forces. The Army's ability to master cloud computing is a critical enabler to the pursuit of leveraging AI and ML in cyberspace warfare. 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 digital overmatch against U.S. near-peer adversaries.

*"... investing in digital transformation and the modernization of the Army's underlying network and computer infrastructure is essential to our success. Specifically, **the cloud is the foundation** for this entire modernization effort. The Army will develop cloud computing technologies, improve data access and sharing environments, and streamline software development tools and services. Together, these technology investments will allow the Army **to take advantage of emerging machine learning and AI technologies** to understand, visualize, decide, and direct faster than our competitors. By leveraging cloud open architecture, information can flow rapidly between the enterprise and soldiers on the ground. This will enable commanders **to counter adversaries in the information environment as effectively as they do in physical domains** and win in the cognitive space."*

— 2019 Army Modernization Strategy

---

<sup>8</sup> On Developing a U.S. Army Enterprise Cloud Strategy, Institute for Defense Analyses; M. Marwick, N. K. Patel, Sept 2019.

## Appendix A: Army Enterprise Cloud Ecosystem Common Services List (IOC)

Below is the initial list of common services that will be provided in Army Enterprise environments. This list will be updated as need dictates.

	<b>Service Name</b>	<b>Service Description</b>
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	Virtual Datacenter Security Stack (VDSS)	All VDSS components and services (e.g. Web Application Firewall, Reverse Proxy, etc.) listed in DISA cloud SRG and SCCA documents, and DoD enclave protection firewall
4	Key Management	PKI certificate signing, administration, and key management
5	Network Infrastructure Management and Monitoring	Monitor, manage, and alert on events related to network utilization and availability
6	DDos Protection Service	Protects applications in the cloud environment from Distributed Denial of Service (DDoS) attacks
7	DNS Hosting, Caching, Recursion	DNS lookup for cloud-based applications and hierarchical DNS management delegated to mission owners
8	PKI Cert Validation	Online Certificate Status Protocol (OCSP) responder to validate if PKI certificates are valid or revoked
9	Network Time	Cybersecurity mandated accurate time source for DoD systems hosted in the cloud
10	Patch Management	Patch repositories for common operating system patch files.
11	SMTP Relay	Simple Mail Transport Protocol (SMTP) based email relay
12	Enterprise Directory Services	Privileged administrative user and non-person entity Identity, Credential, and Access Management (ICAM) (e.g., Active Directory [AD], Lightweight Directory Access Protocol [LDAP])
13	Federated Access Management	User Identity, Credential, and Access Management (ICAM) (e.g., EAMS-A, SAML Services)
14	Secure File Transfer Service (SFTP)	Securely transfer large files to the cloud environment
15	Notification Services	Alerting and notification (e.g., Short Message Service [SMS])

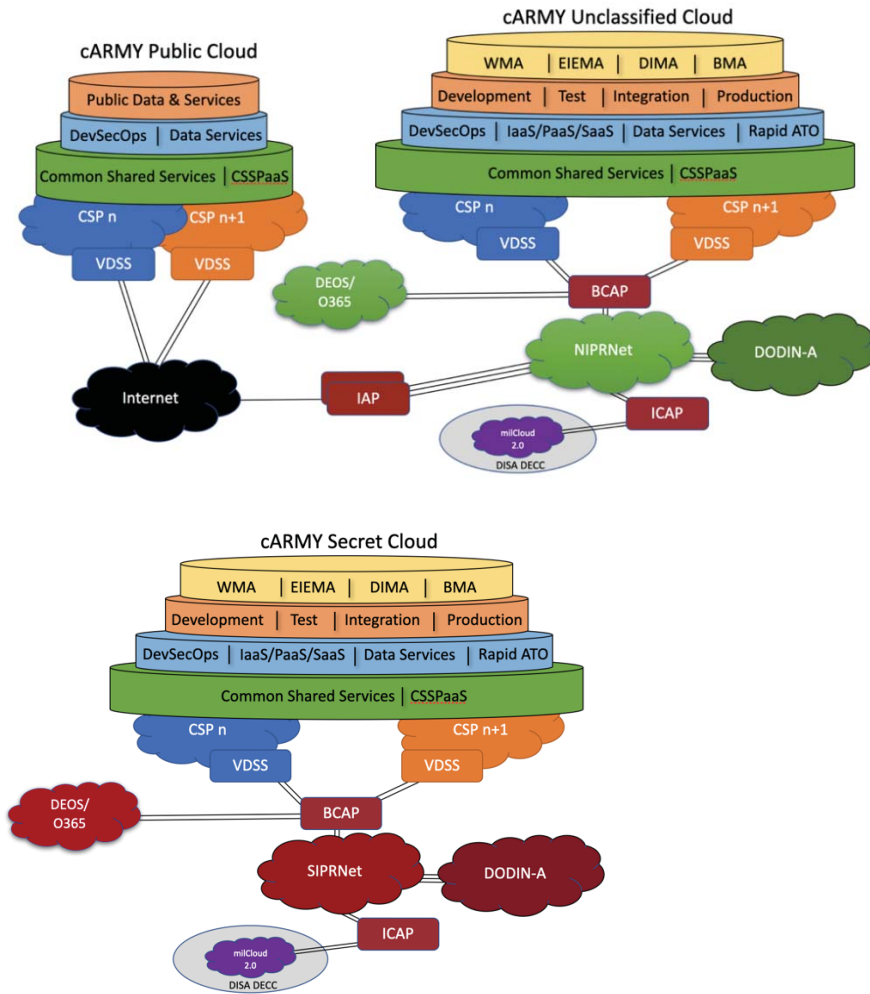
16	Endpoint Monitoring	Protects computing endpoints from malware and other cyber security threats (e.g., Host Based Security Service [HBSS])
17	Remote Privileged Access	Secure administrative access from the Internet or DODIN to DoD servers in secure cloud enclaves.
18	Centralized Logging/Auditing	Consolidated aggregation point for receiving and storing logs from systems and applications in the cloud environment
19	Security Information and Event Management (SIEM) and Log Analytics	Identifies and categorizes security related incidents and events
20	Data Dissemination Service	Accelerates and consolidates data for transfer utilizing secure network tunnels.
21	Code Repository	Code repository for source code configuration management to support a software factory
22	STIG Compliant Virtual Server Templates	A library which stores DISA Security Technical Implementation Guide (STIG) compliant virtual machine template images
23	License/Software Management	Operating System (OS) level license management
24	Asset Management Services	Discover and track assets such as resources, licensed software, etc. within the cloud environment
25	Cross Domain Solution (CDS)	Automatically move appropriately vetted files between security classification levels
26	CSSP Services	Standardized tools & processes to meet cloud cyber security requirements; <i>primarily provided by C5ISR to cARMY tenants. Collaboration with cARMY cloud services ops team</i>
27	Continuous Integration / Continuous Delivery/Deployment (CI/CD) Tools	Tools to enable the CI/CD pipeline (e.g., static and dynamic quality vulnerability load journey integration testing))
28	Enterprise Data Catalog and Service Registry	Data and service listing for data and service management and automated data processing
29	Container Platform	Enabling container runtime services (e.g., container orchestration)
30	Budget and Cost Management	Provides cloud cost and budget information to mission owners
31	Resource Management Portal	Portal to manage compute and store resources

# Appendix B: Army Enterprise Cloud Ecosystem Tiered Services Model

		Infrastructure as a Service (IaaS)		Platform as a Service (PaaS)		Software as a Service (SaaS)	
		Basic	Advanced	Basic	Advanced	Basic	Advanced
Software	Content Management	Content Management	Content Management	Content Management	Content Management	Content Management	Content Management
	Functional Application Management	Functional Application Management	Functional Application Management	Functional Application Management	Functional Application Management	Functional Application Management	Functional Application Management
	Custom/Commercial Software Administration	Custom/Commercial Software Administration	Custom/Commercial Software Administration	Custom/Commercial Software Administration	Custom/Commercial Software Administration	Custom/Commercial Software Administration	Custom/Commercial Software Administration
Platform	DB/Mid Tier Administration	DB/Mid Tier Administration	DB/Mid Tier Administration	DB/Mid Tier Administration	DB/Mid Tier Administration	DB/Mid Tier Administration	DB/Mid Tier Administration
	DB/Mid Tier Platform	DB/Mid Tier Platform	DB/Mid Tier Platform	DB/Mid Tier Platform	DB/Mid Tier Platform	DB/Mid Tier Platform	DB/Mid Tier Platform
	OS Administration	OS Administration	OS Administration	OS Administration	OS Administration	OS Administration	OS Administration
Infrastructure	<b>Virtual Infrastructure</b> DoD/Army Common and Managed Services Virtual Machines VM Network Administration Storage Administration	<b>Virtual Infrastructure</b> Virtual Machines VM Storage Administration VM Network Administration	<b>Virtual Infrastructure</b> Virtual Machines VM Storage Administration VM Network Administration	<b>Virtual Infrastructure</b> Virtual Machines VM Storage Administration VM Network Administration	<b>Virtual Infrastructure</b> Virtual Machines VM Storage Administration VM Network Administration	<b>Virtual Infrastructure</b> Virtual Machines VM Storage Administration VM Network Administration	<b>Virtual Infrastructure</b> Virtual Machines VM Storage Administration VM Network Administration
	<b>Hardware Infrastructure</b> Virtualization Platform Physical Servers Storage Network	<b>Hardware Infrastructure</b> Virtualization Platform Physical Servers Storage Network	<b>Hardware Infrastructure</b> Virtualization Platform Physical Servers Storage Network	<b>Hardware Infrastructure</b> Virtualization Platform Physical Servers Storage Network	<b>Hardware Infrastructure</b> Virtualization Platform Physical Servers Storage Network	<b>Hardware Infrastructure</b> Virtualization Platform Physical Servers Storage Network	<b>Hardware Infrastructure</b> Virtualization Platform Physical Servers Storage Network
		Cloud Service Provided	Army Enterprise Provided	Mission Area Provided			

# Appendix C: Army Title 10 Enterprise Cloud Ecosystem CONUS Common Operating Picture

The picture below represents the Army Title 10 Enterprise Cloud Ecosystem.



- BCAP: Boundary Cloud Access Point
- BMA: Business Mission Area
- CONUS: Continental United States
- CSPaaS: Cloud Service Provider as a Service
- DEOS: Defense Enterprise Office Solution
- DIMA: Defense Intelligence Mission Area
- DODIN-A: Department of Defense Information Network-Army
- EIEMA: Enterprise Information Environment Mission Area
- IAP: Internet Access Point
- ICAP: Internal Cloud Access Point
- VDSS: Virtual Data Center Security Stack
- WMA: Warfighter Mission Area