

Office of the Army Chief Information Officer/G-6

Army Cloud Computing Strategy

MARCH 2015

Enterprise Architecture Division
Army Architecture Integration Center
HQDA CIO/G-6

Version 1.0



CIO/G-6
ENABLING SUCCESS For Today and Tomorrow



CIOG6.ARMY.MIL

UNCLASSIFIED

This page intentionally left blank.

UNCLASSIFIED

TABLE OF CONTENTS

FOREWORD 1

EXECUTIVE SUMMARY 1

1. INTRODUCTION 3

 1.1 Purpose..... 3

 1.2 Scope..... 3

2. CLOUD COMPUTING STRATEGY 4

 2.1 Strategic Context..... 5

 2.2 The Cloud in Context..... 8

3. VISION STATEMENT AND STRATEGIC INTENT 11

 3.1 Vision Statement 11

 3.2 Strategic Intent 11

4. GUIDING PRINCIPLES 14

5. STRATEGIC IMPERATIVES 16

 5.1 Adopt Cloud Governance and Management Practices 16

 5.2 Instantiate Cloud Computing Capabilities within the Army Network 18

 5.3 Manage the Modernization and Migration of Applications, Data and Systems 19

 5.4 Secure and Manage Cloud Operations..... 20

6. ROLES AND RESPONSIBILITIES..... 22

7. CHALLENGES AND MITIGATION..... 23

8. PATH AHEAD..... 25

9. CONCLUSION..... 26

Appendix A References 27

Appendix B Acronyms 31

UNCLASSIFIED

This page intentionally left blank.

UNCLASSIFIED

FOREWORD

In support of a globally responsive and regionally aligned force, the Army is working with key mission partners to implement a cloud-enabled network. The Army will implement modernization plans and develop processes and procedures to leverage approved DoD, federal and commercial cloud service providers. The Army will ensure offerings align with mission requirements and provide the minimum set of security controls necessary to protect critical information against known and emerging threats.



LTG Robert S. Ferrell
Chief Information Officer/G-6

Transitioning to cloud-based solutions and services advances the Army's long-term objective to reduce our ownership, operation and sustainment of hardware and other commoditized information technology (IT). Procuring these as services will allow the Army to focus resources more effectively to meet evolving mission needs. Over time, it also will significantly boost IT operational efficiency, increase network security, improve interoperability with mission partners, and posture the Army to adopt innovative technology more quickly at lower cost.

Preparing for this dynamic shift in the way the Army develops, acquires and delivers IT capabilities and services comes with significant challenges and inherent risks. The Army must ensure that it does not compromise its mission by unrealistically trading the confidentiality, integrity and availability of critical data and information in pursuit of the benefits the cloud may offer. The potential vulnerabilities of, and impacts, to expeditionary operations in highly contested and inevitably degraded communication environments must be carefully and continuously assessed and weighed against the advantages of adopting cloud technologies.

To support the move to a cloud computing environment, investments are required to both improve the capacity and security of network infrastructure and to modernize, prepare and migrate applications. Executing such a dramatic, yet very necessary, shift requires the synergy and support of every corner of our Army.

The Army's Cloud Computing Strategy and the Army's Network Campaign Plan, along with the Army's Implementation of the Intelligence Community Information Technology Enterprise (IC ITE) cloud strategy and other key strategic documents, outline efforts that posture the Army for success in a complex world. The transition to cloud-based solutions and services will enable the Army to successfully provide the robust network necessary for our warfighters anytime, anywhere.

A handwritten signature in black ink, appearing to read "Robert S. Ferrell".

Robert S. Ferrell
Lieutenant General
Chief Information Officer/G-6

UNCLASSIFIED

This page intentionally left blank.

UNCLASSIFIED

EXECUTIVE SUMMARY

The Army Cloud Computing Strategy establishes and communicates the Army's vision and strategy for delivering cloud-enabled network capabilities to improve mission and business effectiveness, increase operational information technology (IT) efficiencies and protect Army data and infrastructure. The Army Cloud Computing Strategy extends the baseline and concepts defined in the various federal, DoD, and Army policies and documents and is nested with the Army Network Campaign Plan.

The Army's IT infrastructure is made up of systems, software and application platforms, data assets, and related business processes and practices. This strategy provides guiding principles, challenges and mitigation plans for transitioning the Army's current IT infrastructure from traditional development and deployment approaches to a consolidated computing approach via cloud-based IT service delivery solutions and models within the guidelines of the mission-focused cloud security model.

Cloud infrastructure, people and processes will be central to enabling the Joint Information Environment (JIE) [33] and the Intelligence Community Information Technology Enterprise (IC ITE) [5]. Cloud computing has demonstrated the potential to change the responsiveness of capabilities supporting the generating and operating Forces and unified action partner (UAP) operations across all joint operational phases – Shape, Deter, Seize Initiative, Dominate, Stabilize, Enable Civil Authorities – whether preparing to deploy in the installation IT environment, conducting home-station mission command, en route or engaged as part of a Joint force in a theater of operations. The ability to connect to cloud capabilities assures that Army computing and communications resources, authoritative data sources, services and information are available, accessible and safeguarded, from the enterprise to the edge.

A solid data foundation is critical for executing a cloud-based enterprise data strategy that provides trusted information to decision makers. The ability to maximize discovery and understanding of data promotes cost efficiency and greater effectiveness. With the implementation of a cloud-enabled network, the Army will fully realize the efficiencies of the JIE and the Common Operating Environment.

The Army is changing its approach to modernizing information technology (IT) infrastructure by moving to a cloud based approach. This approach emphasizes reducing IT hardware procurements and sustainment in favor of procuring these capabilities as services from cloud providers.

Achieving gains in efficiencies and effectiveness from cloud computing will require deliberate synchronization and integration across numerous organizations both within and external to the Army. Securing Enterprise-wide commitment, planning and coordination across multiple technologies, programs of record, business practices and workforce dimensions are required to move from today's independently owned and managed IT infrastructure, systems and databases to a more standardized, centrally managed cloud-enabled network. To facilitate full unity of effort, this strategy identifies four strategic imperatives (Adopt Cloud Governance and Management Practices; Achieve an Army Cloud-Enabled Network; Manage the Modernization and Migration of Applications, Systems and Data; and Secure and Manage Cloud Operations) and associated enabling objectives. These imperatives are intended to drive the Army's transition to cloud-enabling capabilities and to synchronize planning, resourcing and acquisition activities in the institutional and operational environments.

The Army will build the foundation for transitioning to cloud enabled capabilities by focusing on improving data security, network security and throughput – the amount of information passing through the system – to ensure that sufficient capacity exists for authorized users to securely

access and work within the cloud. Simultaneously, the Army will continue rationalization of existing systems, applications and associated data as part of on-going portfolio management efforts while determining the most appropriate cloud service/deployment model for migration. Through the Army Application Migration Business Office [6], the Army intends to rapidly capitalize on the Federal Risk and Authorization Management Program (FedRAMP) [7] and DoD-approved government and commercial cloud service providers (CSP) to the maximum extent feasible. Application and system migration decisions must be based upon an evaluation of risk to the mission resulting from a potential loss of access to, or the compromise of the integrity or confidentiality of, information. Generally, migration will improve cybersecurity, reduce sustainment and operating costs, improve the efficiency of contracting resources, shorten implementation timelines, and more effectively keep pace with emerging technologies while taking advantage of the larger economies of scale that typically reduce costs.

Federal cloud computing is still in an early deployment stage. The Army anticipates periodically updating the Cloud Computing Strategy and associated architectures to reflect maturation of standards and policies and lessons learned during implementation. As the network aggregates, processes, secures and presents data in a way that is easily understood, Soldiers will be able to make informed, more effective decisions as they perform the missions of the future. The end state is a global cloud-based environment designed to provide Soldiers access to tailored and timely information at the point of need.

1. INTRODUCTION

1.1 Purpose

The purpose of this document is to formalize and communicate the Army's strategy for leveraging a cloud computing environment, where appropriate, to improve mission and business effectiveness and increase operational information technology (IT) efficiencies, while accounting for new and evolving threats. This strategy also serves as the basis for development of more detailed implementation plans. Additionally, it describes a path forward to realize Army and DoD leadership objectives of reducing the costs associated with IT operation and maintenance, more easily deploying new technology and improving the security posture of Army applications on the network.

The Army Cloud Computing Strategy supports:

- The Federal [1] and Department of Defense (DoD) [2] *Cloud Computing Strategies*
- The DoD Joint Information Environment (JIE) [33]
- The DoD Chief Information Officer's *DoD Cloud Way Forward* [32]
- *Army Network Campaign Plan 2020 and Beyond* [4] and implementing guidance
- The Intelligence Community Conceptual Architecture [5]
- The Assistant Secretary of the Army (Acquisition, Logistics and Technology) *Common Operating Environments (COE) Data Center/Cloud Computing Environment (DCCE) Architecture* [9]
- NIST SP 800-144, NIST Guidelines on Security and Privacy in Public Cloud Computing [31]
- The DoD Cloud Computing (CC) Security Requirements Guide (SRG) [18]

As federal cloud computing is still in an early deployment stage, the Army anticipates periodically updating this strategy and associated architectures to reflect maturation of standards and polices throughout DoD.

To facilitate full unity of effort, this strategy identifies four strategic imperatives:

1. Adopt Cloud Governance and Management Practices
2. Instantiate Cloud Computing Capabilities within the Army Network
3. Manage the Modernization and Migration of Applications, Systems and Data
4. Secure and Manage Cloud Operations

These four imperatives must be continually assessed and mutually synchronized with each other. Each imperative includes associated enabling objectives, which are intended to drive the Army's transition to the cloud and synchronize planning, resourcing and acquisition activities at the institutional and operational levels. The adoption of cloud computing technologies and solutions requires significant change; therefore, a section on challenges and mitigations is included.

1.2 Scope

This document clarifies the strategic intent, provides guiding principles and identifies strategic imperatives and enabling objectives to transition the Army to cloud computing within all defined COE computing environments, where appropriate. This document will serve as the basis for future planning and implementation. This strategy references the key documents and initiatives that are core to implementation, providing the reader a convenient way to gather additional information that is beyond the scope of this document.

2. CLOUD COMPUTING STRATEGY

The Army Cloud Computing Strategy sets the strategic direction and guidance to posture the Army for maintaining a secure operating environment while transitioning the Army's IT infrastructure, systems, software and application platforms; data assets; and related business processes and practices.

It represents a move from traditional development and deployment methodologies to a consolidated management approach for delivery of secure, scalable and reliable cloud-based IT services, solutions and deployment models.

Successful migration to cloud computing technologies and solutions touches and depends upon numerous ongoing Joint and Army initiatives, which must be fully synchronized. These include major modernization efforts such as:

- Deployment of the Defense Information Systems Agency's (DISA) milCloud [8]
- Adoption of Multiprotocol Layer Switching (MPLS) and other infrastructure upgrades to increase capacity of the core and installation transport capability
- JIE cybersecurity architecture through the Joint Regional Security Stacks (JRSS)
- IC ITE Enterprise Services (e.g. Enterprise Management Tools, Apps Mall, etc.) [5]
- Enterprise Identity and Access Management (IdAM)
- Implementation of the Army's COE Architecture – Annex B, Definitions and Guidance for the COE to the LandWarNet 2020 and Beyond Enterprise Architecture [10]
- Training and Doctrine Command (TRADOC) Pamphlet (TP) 525-3-1, The U.S. Army Operating Concept (AOC), 7 October 2014 [30]
- Delivery of enterprise services (e.g., enterprise email, Unified Capabilities (UC), web portal, etc.) and applications (e.g. GFEBs and GCSS-A).
- Consolidation and standardization of computing, hosting and storage infrastructure through the Army Data Center Consolidation Plan (ADCCP) [6]

Because these initiatives and activities are not all under the control of a single DoD component, this transformation requires a unified management approach and must be based on IC, Joint and Army support concepts. By its very nature, this transformational shift requires the synergy and support of:

- Army Headquarters Staff
- Program Executive Officers (PEOs)
- Army Application Migration Business Office - Product Director Enterprise Computing (PD EC)
- Program Managers
- Army Commands
- Army Service Component Commands
- Direct Reporting Units
- Office of Business Transformation
- Reserve Components of the Army

The Army also must closely consult and coordinate with numerous external entities, including the DoD Chief Information Officer, Defense Information Systems Agency (DISA), the Intelligence Community and other DoD components and agencies.

2.1 Strategic Context

The Joint Chiefs of Staff and the DoD CIO brought the Service components and DISA together to create and manage the JIE [33]. The goal of the JIE is to establish a single, secure information environment that enables commanders to connect to, access and share the information they need in order to operate effectively. Cloud-based capabilities are key to the JIE's success; they will allow consolidation of applications and core capabilities in secure environments, and universal accessibility across DoD and the Army. The DoD CIO, DISA and Service components have established ongoing collaborative forums and working groups to ensure that the DoD Cloud Strategy and related implementation guidance and architectures are aligned to deliver innovative, efficient and secure cloud-enabling infrastructure and services consistent across the JIE.

The Army must improve efficiency and reduce costs while maintaining data security associated with hosting and supporting the large number of software applications and systems currently, and projected to be, in use. As part of the ADCCP [6], the Army must consolidate hundreds of Army data centers into standardized Core Data Centers, Installation Processing Nodes and/or non-DoD cloud service provider (CSP) facilities, as appropriate. Army commands, staff, mission areas and domain managers must determine whether to sustain, kill or modernize their applications. Enduring applications must then migrate to an approved hosting environment. The Army must also ensure that capabilities provided by existing Mission Command systems, such as Warfighter Information Network-Tactical (WIN-T), Distributed Common Ground System-Army (DCGS-A), Command Post of the Future (CPOF), and the Advanced Field Artillery Tactical Data System (AFATDS) maintain interoperability and interconnectivity with stakeholders internal and external to the Army.

Figure 1 illustrates various corresponding strategies and papers that are driving creation of cloud-based capabilities that support the Army Concept of Operations. As these activities and initiatives materialize, the Army's Hybrid Cloud capability will be realized.

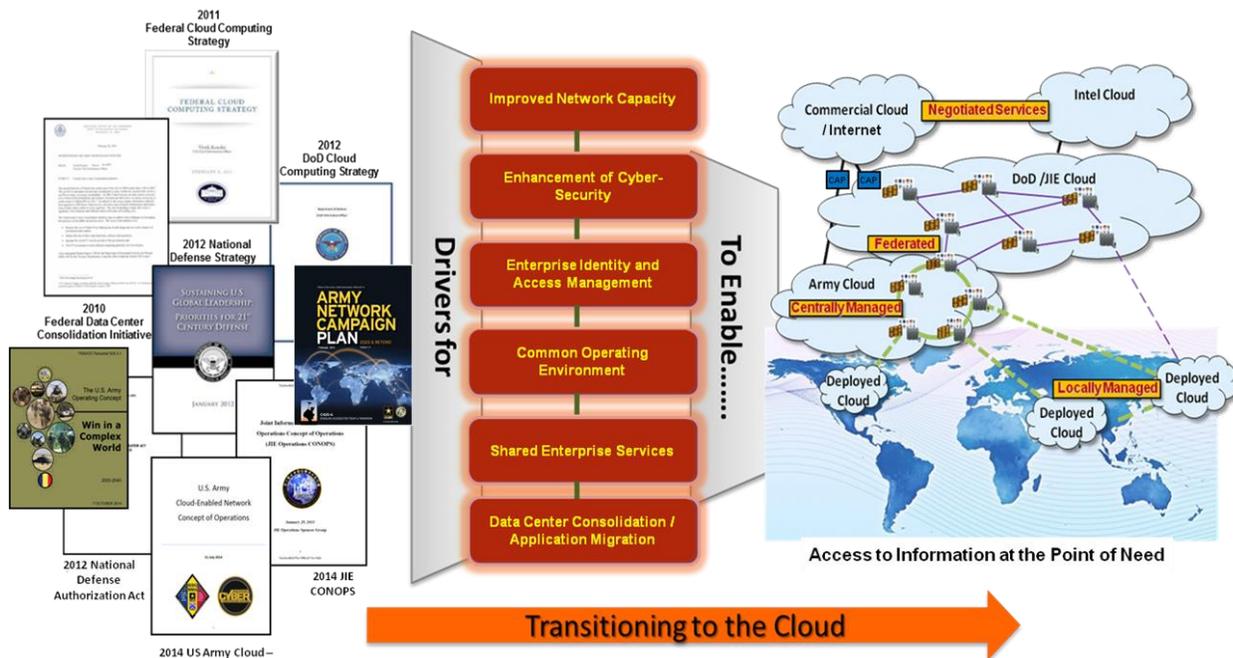


Figure 1: Cloud Computing Strategic Context

Another key motivation for the adoption of cloud computing is the demonstrated success with cloud computing within the private sector. This success comes from innovations and key technology breakthroughs that facilitate:

- Widespread availability of affordable high-speed bandwidth
- Smaller, more powerful and cheaper computer processors and end-user devices
- Parallel processing methodologies
- Rapid software deployment cycles
- Improved virtualization of data storage and processing capabilities allowing multiple applications to run simultaneously on shared physical resources
- Enhanced data center automation, which significantly reduces requirements for system administration labor
- Near-universal software interoperability standards
- Creation of new online marketplaces where software platform providers, device manufacturers, application developers and consumers can interact

Adoption of these advances sets the conditions for the ADCCP to transition the collecting, accessing, processing and distributing of information, data and applications from individual desktops, laptops or local server rooms to centrally managed remote data centers. When data center consolidation is combined with a cloud computing, utility-based model for buying and selling IT capabilities and services, aggregation and delivery of on-demand, pay-for-use services to customers becomes an attractive and highly competitive business opportunity. At the same time, a methodical process that accounts for evolving security and operational concerns, based upon risk-informed assessments, must be instituted.

All of these factors help make cloud computing an option that provides significant cost savings, IT efficiencies and improved capability delivery. As described by National Institute of Standards and Technology (NIST) Special Publication SP800-145 [13], cloud computing is a model composed of five essential characteristics.

- 1) *On-demand self-service*, where consumers can rapidly provision and release services with minimal management effort or service provider interaction.
- 2) *Broad network access* to capabilities through standard mechanisms that enable dissimilar devices (e.g., mobile phones, tablets, laptops and workstations).
- 3) *Resource pooling* of configurable computing resources (e.g., networks, servers, storage, applications and services).
- 4) *Rapid elasticity*, where computing resources, often appearing unlimited to the user, can rapidly scale up or down commensurate with demand.
- 5) *Measured service* to monitor, report and automatically control and optimize resource usage through a metering capability at some level of abstraction (e.g., storage, processing, bandwidth and active user accounts).

Determined to take advantage of the cloud's IT efficiencies and business improvements, in 2010 the U.S. Federal Government CIO released the *25 Point Implementation Plan to Reform Federal Information Technology Management* [14]. Aimed at fundamentally changing the way federal agencies spend and subsequently manage approximately \$80 billion in IT expenditures each year, the plan launched a "Cloud First" policy, mandating the use of cloud-based solutions to the maximum extent possible. In rapid succession, the White House, Congress and DoD issued subsequent guidance with the intent of accelerating the government's transition to cloud computing, specifically, the 2011 Federal Cloud Computing Strategy, the fiscal year 2012 National Defense Authorization Act and the 2012 DoD Cloud Computing Strategy. Cloud services will not be appropriate for all applications and some anticipated benefits may not be

achieved to the same degree as others. During design and implementation, overall risk and benefits must be managed in a way to maximize the overall value of the solution. Most often, the most desired benefit is lower overall cost, and the expectation is an almost immediate reduction in cost; however, these expectations generally do not materialize during the initial modernization and migration period. Although application owners and commands will require additional upfront investments for migration, the Army is expected to realize long-term reductions in overall infrastructure costs. When designed and implemented properly, in addition to the benefits identified above, a cloud computing architecture should

- Simplify infrastructure updates, operation and maintenance
- Simplify various IT functional areas
- Simplify operating system updates on applications (PaaS/SaaS)
- Improve network resiliency through more consistent security implementations, effective load balancing and removal of single points of failure throughout the enterprise
- Increase purchasing power through economies of scale and commoditization of IT services
- Support private multi-tenancy operations with DoD partners, which enables data aggregation for analysis and re-use of applications
- Raise the potential for better interoperability with DoD mission partners
- Allow portability of services from one provider to another
- Improve the flexibility and scalability to expand computing power as required to support growth
- Make application deployment more agile
- Improve future planning and service continuous-improvement through the availability of metrics and predictability of a standardized service delivery environment

Careful consideration of the effects on Mission Command during en route mission planning, forces operating in highly contested and disconnected, intermittent or low-bandwidth (DIL) environments, cybersecurity and legal jurisdictions must be weighed along with the potential benefits of using cloud technologies. Implementation plans and Service deployment models for forward-based and tactical applications must support DIL requirements, as noted in the *U.S. Army Cloud-Enabled Network Concept of Operations* [11]:

“... the challenges for cloud-enabled networks are most severe in terms of capacity and connectivity. Operational factors limit bandwidth availability resulting in frequent DIL conditions.... Cloud architecture must allow individuals and units to disconnect from the network, continue to conduct operations, and then reconnect and resynchronize with the network as connectivity is restored.”

In order to mitigate risk in these conditions, mission-critical capabilities will require lightweight tools that can operate in a DIL environment and synchronize as necessary within the greater architecture.

For applications and data identified for migration to the cloud, commands and application owners must analyze and right size their application hosting requirements [6], thereby ensuring that the Army buys only what is needed (rather than moving to the cloud environment with over-provisioned applications). Application owners must collect performance data to support this level of engineering analysis. The Army Application Migration Business Office – Product Director Enterprise Computing, will assist commands with the system planning required to move applications to the cloud. Additionally, application and system migration decisions must be based upon a approved business case analysis (BCA) in accordance with the DOD CIO

direction contained in the Updated Guidance on the Acquisition and Use of Commercial Cloud Computing policy memo [34] and forthcoming Army CIO/G6 BCA implementation guidance. In addition, an evaluation of risk to the mission resulting from loss of access to, or the compromise of the integrity or confidentiality of, information must be taken into consideration.

2.2 The Cloud in Context

NIST defines cloud computing as "... a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." For the Army cloud-enabled network, the desired end state includes enabling, as much as possible, the characteristics of cloud as described in NIST Special Publication 800-145[13].

Most generic definitions of the cloud end at this level; however, the Army Data Center Computing Environment (DC CE) Architecture [9] and the U.S. Army Cloud-Enabled Network Concept of Operations [11] further define and detail the specific services that the cloud must provide in order to achieve the Army's vision.

Cloud service model: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). This element shows the services being procured from a CSP. Figure 2 depicts each of the different cloud service models and which components are managed directly by the application or system owner (consumer) or purchased as a service from the CSP. It is crucial that the community understand not only the service being provided but also what the consumer must continue to maintain in relation to what the CSP will maintain. The IaaS, PaaS, and SaaS do not change the necessary service delivery components of the cloud service model but, rather, what is being bought as a cloud service.

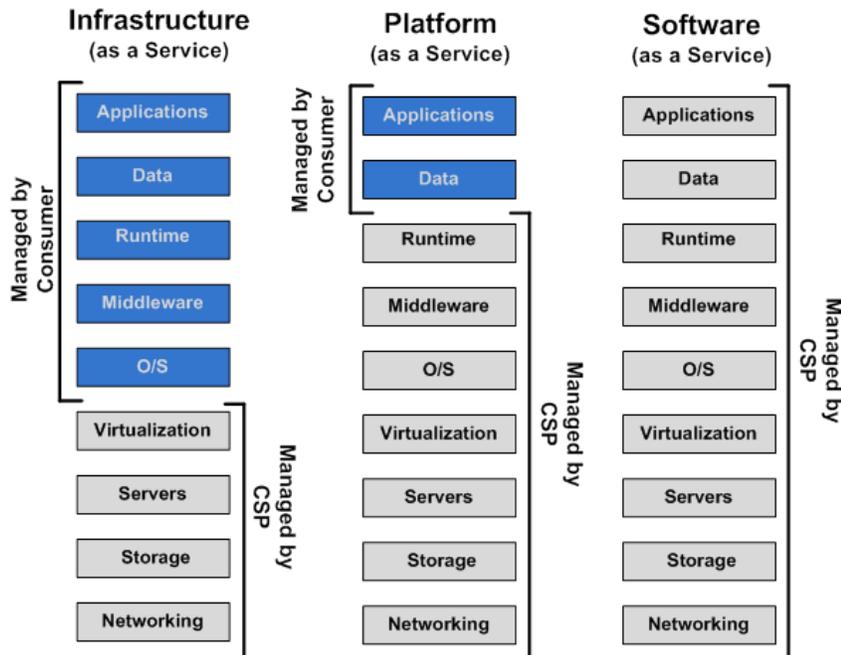


Figure 2: Cloud Service Model

Cloud deployment model: private, community, public or hybrid. This element communicates how the CSP will host the service and related data, and is described in NIST Special Publication 800-145 [13]. For the Army, the deployment model is important due to DoD cybersecurity

requirements and limitations regarding where DoD data can be hosted in accordance with applicable federal law. Appropriate deployment models will be selected after careful evaluation using the DoD Risk Management Framework (RMF) [17], the special considerations outlined in NIST 800-144 [30] and careful consideration of the various levels of data sensitivity as described in DoD Cloud Computing Security Requirements Guide (CC SRG) [18] (see Table 1) and the mission criticality of the system or application.

Information Security Impact Levels		Definitions
CSM	CC SRG	
1	2	Unclassified, publicly releasable information, e.g., recruiting websites
2		Unclassified, publicly releasable information with access controls, e.g., library systems
3	4	Non-National Security System (non-NSS) Controlled Unclassified Information (CUI) – low confidentiality impact, moderate integrity impact, e.g., training systems
4		Non-NSS CUI – moderate confidentiality impact, moderate integrity impact, e.g., human resource systems, personally identifiable information (PII), and protected health information (PHI)
5	5	NSS CUI – moderate confidentiality impact, moderate integrity impact, e.g., email systems
6	6	Classified information up to and including Secret – moderate confidentiality impact, moderate integrity impact, e.g., command and control systems

Table 1: Security Levels

Table 1 above encompasses most elements of the Army enterprise IT portfolio, but Army Intelligence maintains data classified above the Secret level and must comply with Intelligence Community requirements to secure data above Level 6.

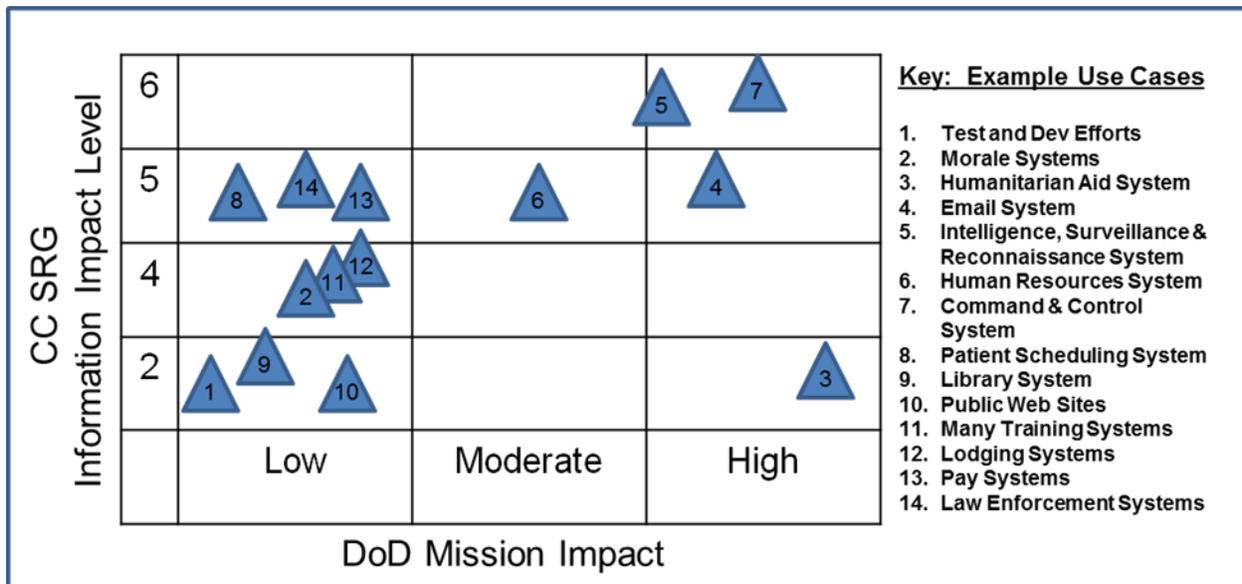


Table 2: Mission-focused System Categorization

Table 2 above provides example mappings of capabilities to the security impact levels. Using this table, mission owners can identify where their capability might be hosted in the Army hybrid cloud.

Table 3 describes the various cloud computing deployment model considerations within the network. The Army Application Migration Business Office - PD EC can assist with determining the most appropriate deployment model based on risk and approved CSPs.

Army Cloud Computing Deployment Models						
On-Premise (DoD Network & Facilities)			Off-Premise (Non-DoD Federal or Commercial Facilities) <small>* Must be within defined US Jurisdictional areas Only</small>	Off-Premise (Non-DoD Federal or Commercial Facilities) <small>* Must be within defined US Jurisdictional areas Only</small>	Operationally Deployable	
Gov't Owned Gov't Operated	Gov't Owned Cml Operated	Cml Owned Cml Operated	Federal Tenants Only	Multi-Tenant	Army Tactical Infrastructure	
DoD Community Cloud			Federal Community Cloud	Public / Federal Community Cloud	DoD Community / Army Private Cloud	
CC SRG Impact Levels up to 6			CC SRG Impact Levels up to 6	CC SRG Impact Levels up to 4	CC SRG Impact Levels 4 to 6	

Table 3: Cloud Computing Deployment Models

3. VISION STATEMENT AND STRATEGIC INTENT

3.1 Vision Statement

By 2025, the Army will continue to maintain a strategic and tactical advantage over its adversaries through information dominance by fully leveraging an optimal mix of approved government and commercial cloud service providers that globally support Total Force requirements for quality of service. Cloud computing, when coupled with the appropriate applications and a common data structure, will enable authorized users to harness the power of Big Data analytics through a COE that enables low-latency access to required data elements, regardless of location or device. Moreover, these data elements will be customizable to the desired format of mission commanders, senior leaders, decision makers and other authorized mission partners.

In order to achieve the cloud computing vision, the Army will start building the foundation by focusing on improving network security and throughput to ensure that sufficient capacity exists for tactical edge users to access and securely work within the cloud. Simultaneously, the Army will continue its emphasis on the rationalization of existing systems, applications and associated data (i.e., the use of authoritative data sources) while determining the most appropriate cloud service and deployment model for migration and improving secure mobile computing capabilities. The Army intends to rapidly capitalize on Federal Risk and Authorization Management Program [7] and DoD-approved government and commercial CSPs to the extent that doing so aligns with mission requirements without compromising security. This will reduce the amount of contracting and cybersecurity resources required, shorten implementation timelines, and more effectively keep pace with emerging technologies. In some instances, particularly when an application processes classified data (e.g., Secret and above), the Army may need a private cloud infrastructure either in its own facilities or other DoD facilities that have been certified and approved to process data at the appropriate classification level

3.2 Strategic Intent

Cloud computing will increase capabilities and responsiveness of the operating force and UAPs globally during all joint operational phases (Shape, Deter, Seize Initiative, Dominate, Stabilize, Enable Civil Authority), whether they are preparing to deploy in the installation IT environment, en route or engaged as part of a Joint force in a theater of operations. Cloud infrastructure, people and processes will be central to enabling the JIE. The ability to connect to cloud capabilities assures that Army computing and communications resources, services and information are available, accessible and safeguarded from the enterprise to the tactical edge in a cloud environment across all security domains. (For more information defining UAP, refer to Army Doctrine Reference Publication -30, Unified Land Operations.) [12]

Going beyond infrastructure consolidation, the Army's intent is to implement cloud computing as the means to deliver the most innovative, efficient and secure information and IT services in support of "the department's mission, anywhere, anytime, on any authorized device" (DoD CIO *Cloud Computing Strategy*, July 2012) [2]. This will reduce Operations and Maintenance (O&M) costs by decreasing the overall investment in hardware and software assets, leveraging economies of scale and automating the monitoring and provisioning of service delivery and assurance. Additionally, this postures the Army to stay current with evolving technology with limited impact to the end user (upgrades are made seamlessly behind the scenes), while supporting the management of resources according to mission priorities. Enabled through the Army's standardized COE and implemented through the Army Application Migration Business Office and DISA, the Army will simplify and extend access to timely and relevant data,

applications, collaboration tools and other managed services through the cloud. Ultimately, the Army Cloud Computing Strategy way ahead will be integrated with a comprehensive approach to enable horizontal and vertical interoperability between all Mission Command systems, across echelons and with stakeholders external to the Army.

A critical component of *The Army Network Campaign Plan 2020 and Beyond* [4] is to employ cloud technology to provide users access to data and applications over the network from centrally managed enterprise computing and storage locations while enabling local cloud deployments to support critical operational needs. This aligns with federal and DoD strategies to leverage commercial cloud technologies wherever practicable and private government clouds when appropriate, and to deploy local clouds as necessary to achieve mission objectives.

Moving to cloud-based solutions and services:

- Supports the JIE [33] by providing capability in centralized locations that are accessible across the DoD Information Network (DoDIN).
- Advances the Army's long-range objective of transitioning away from owning, operating and sustaining hardware and other commoditized IT in order to better focus its resources to meet evolving mission needs.
- Supports Army Mission Command Network 2020 Focused End State 4.0 (joint, interagency, intergovernmental and multinational interoperability with UAPs).
- Supports the ADCCP [6], which will leverage cloud technology to reduce costs, consolidate capabilities, systems and applications, and provide central accessibility to the enterprise.
- Provides a platform for the creation of standard solutions and efficiencies that can be applied consistently to ensure both capabilities and cybersecurity are effectively implemented seamlessly across the institutional and operational environment.
- Provides an infrastructure that supports more agile and faster implementation of new systems.
- Provides flexibility by using automation to expand or contract application resources based on utilization.

Achieving the intended outcomes above and related gains in efficiencies and effectiveness from cloud computing will require deliberate synchronization and integration across numerous organizations both within and external to the Army. This necessitates a strong governance process, adherence to policy and close coordination with the Army Application Migration Business Office by organizations migrating applications and systems. The Army will continuously assess and weigh the potential benefits of various cloud deployment models against potential risks, such as:

- Increased technical complexity
- System performance and outages
- Competitive, congested and contested cyber electromagnetic environment
- Data storage and information security
- Changes in vulnerability attack vectors
- Government data storage legal compliance

While deploying cloud solutions in an enterprise as large and diverse as the Army is inherently complex, the governance, architectural, technical and funding challenges become increasingly magnified as we align, integrate and execute as part of the JIE, the Intelligence Community Information Technology Enterprise (IC-ITE) [5] and, as required, with other domestic agencies and mission partners. Ensuring that Army mission needs are met and enhanced hinges on having a solid yet flexible strategy that informs trade space decision making; an enterprise

architecture that addresses unique Army operational requirements; and the knowledge and expertise necessary to negotiate and manage a utility-based business model.

Over time, applicable applications, systems and operations will be transitioned to CSPs. This will significantly boost IT operational efficiencies and effectiveness, and ultimately position the Army to more quickly adapt innovative and emerging capabilities, such as advanced Big Data analytics, that will provide decision makers a clearer understanding of the environment.

4. GUIDING PRINCIPLES

The guiding principles associated with cloud computing are precepts, rules or fundamental ideas that provide overall Army direction to commands, program managers and/or application owners. The following principles embody the key ideas that shaped the development of the Army Cloud Computing Strategy and will continue to guide decisions during its implementation.

- **Common standards** – The design and use of the Army cloud will follow approved JIE, LandWarNet 2020 [19], cloud architecture[9][29], Army Information Architecture [20] and operational directives to ensure the maximum level of interoperability across multiple CSP hosting environments, using common data normalization and application program interface standards. This ensures that Army applications and data will be modernized and optimized to provide maximum interoperability with other DoD components and mission partners.
- **Enable resilience through dynamic security** – Resilience means being able to continue operations in the face of a threat or system failure. Dynamic security requires the continuous monitoring and evaluation of systems, capabilities, interfaces, applications and data transactions to assess threats to cybersecurity and risks that may affect confidentiality, integrity and availability.
- **Use the appropriate deployment model** – Data and systems are categorized into several different levels. Each level comes with its own set of requirements as described in the Cloud Computing SRG [18]; lower impact levels are less restrictive than higher impact levels. Services must be acquired in a sensible manner, protect data according to the highest impact level and leverage multiple clouds when efficiencies can be achieved (e.g., leverage off-premise commercial cloud offerings for data impact levels 1-5 and on-premise private cloud for up to level 6).
- **Cybersecurity Cloud protection** – Data and systems must be protected from both external attackers and insider threats. Security countermeasures must be integrated from the beginning, protecting each element of the data, tracking provenance and matching each user's roles and authorizations against each data security label to ensure that users and applications access only the data for which they are authorized. Provenance must enable auditing and dynamic forensic analysis to identify all users, products and processes that used the data; protect against cyber attack; and respond following any unauthorized disclosure of information. The cloud will maintain the security posture required to protect data and meet the Army's mission requirements.
- **Lower IT costs** – The economies of scale created through aggregated common infrastructure, licensing, increased automation, the transfer of technology costs from capital to operational expense, the shift to paying for what is used when it is needed, higher computational density and lower power requirements lead to lower overall costs (following the initial investment required for migration). Additionally, the emphasis on right-sizing application requirements and designing them to leverage a virtual environment ensures that requirements are not over-provisioned, and only the minimum capabilities required to operate are procured.
- **Greater agility** – Faster and simpler access to scalable infrastructure services, software platforms and enterprise software services increases responsiveness to new and evolving mission and business needs, and allows application developers to rapidly deploy capabilities into enterprise operations.
- **Service delivery under DIL conditions** – The ability to create and process mission-critical data locally while disconnected from the cloud and synchronize that data once reconnected is a critical element to fully enabling the operating force during en route mission planning and operations in highly contested and DIL environments. Cloud technologies and applications adopted and employed for the lower tiers of the enterprise, such as operational

and tactical formations, must account for this requirement through off-line data synchronization for high-risk data that will be leveraged through the cloud by other entities of the force.

- **Minimization of redundant data sources** – The use and reuse of defined authoritative data sources and standard data services provide access to cost-effective structured and unstructured data through simplified interfaces. Improved data quality is achieved by performing functions such as eliminating duplication, consolidation and tagging of all data in cloud environments. Army Intelligence data resources will continue to comply with Intelligence Community data governance standards and requirements.
- **Interoperability & portability** – Compliance with the Army Information Architecture [20], data standards and common syntax reduces translation and mediation, and ensures interoperability of applications and data for effective information sharing among Army, UAPs and DoD mission partners. This principle also ensures that Army information assets are able to move seamlessly between infrastructure workloads and from one CSP to another to provide a common user experience. (See also Department of Defense Information Network Cloud Computing Services Interoperability and Portability Reference Architecture.) [21][20].
- **Mission effectiveness** – The Army must ensure that it does not compromise its mission by unrealistically trading the confidentiality, integrity and availability of critical data and information in pursuit of the benefits the cloud may offer. The potential vulnerabilities of and impacts to expeditionary operations in highly contested and inevitably degraded communication environments must be carefully and continuously assessed, then weighed against the advantages of adopting cloud enabling capabilities.

5. STRATEGIC IMPERATIVES

Moving from today's independently owned and managed IT infrastructure, systems and databases to a more standardized, centrally managed cloud computing environment is a complex endeavor requiring enterprise-wide planning and coordination across multiple DOTMLPF-P areas, technologies, programs of record, business practices and workforce dimensions. The IT considerations are wide ranging and include server virtualization, network bandwidth modernization, application redesign, data management modernization, service automation and enhanced cybersecurity. The impact on the Army's workforce will extend beyond our IT occupational specialists to include our acquisition, business, functional mission owners and users. New procurement, management and funding practices that focus on responsive and enforceable service level agreements (SLAs) will be required. SLAs are used to address DoD and Army requirements, and the general recommendations in NIST SP 800-146 [22], for management, data governance, security and reliability, virtual machines, software and applications.

To accomplish the transition, there are four strategic imperatives and associated enabling objectives necessary for delivery of capabilities to warfighters and support to critical business functions.

- Adopt Cloud Governance and Management Practices
- Instantiate Cloud Computing Capabilities within the Army Network
- Manage the Modernization and Migration of Applications, Systems and Data
- Secure and Manage Cloud Operations

Multiple enabling objectives and underlying actions have been identified to support each of the identified imperatives and are aligned to the Army Network Campaign Plan. These objectives need to be achieved for the Army to successfully migrate and adapt to a cloud-enabled network environment.

5.1 Adopt Cloud Governance and Management Practices

This imperative aligns to the ANCP Lines of Effort (LOEs) Provide Signal Capabilities to the Force and Strengthen Network Operations.

➤ Enabling Objective 5.1.1: Synchronize planning, resourcing and acquisition activities

- Leverage the Army CIO/G-6 Integrated Process Team (IPT) for Application Hosting (IPT 1) and ensure maximum participation and accountability.
- Formulate and defend resources necessary to deploy cloud enabling capabilities in accordance with the roadmaps identified in the *Army Network Campaign Plan 2020 and Beyond* [4] and implementing guidance
- Continue to maintain a single Army Application Migration Business Office – PD EC within Program Executive Office Enterprise Information Systems to assist system/application owners with modernization and migration requirements, determine the most appropriate cloud deployment model, and negotiate and acquire cloud capabilities from approved CSPs.
- Collaboratively develop and implement the Army COE and required changes across doctrine, organization, training, materiel, personnel, leadership and professional development, facilities and policy (DOTMLPF-P).
- Define and implement cloud computing return on investment models, key performance indicators and metrics to measure, accurately predict and monitor the effective adoption of the technology.

- Incorporate migration resourcing requirements *early* in the Program Objective Memorandum process to ensure programming availability and alignment with migration plan timeline.
- Provide key artifacts for resource validation by command resource managers, Management Decision Evaluation Package managers, Program Evaluation Group (PEG) panels, etc.
- Develop standard contractual terms and conditions and service level agreements.
- Leverage pre-negotiated terms and pricing at the DoD and Army enterprise levels through the Army Application Migration Business Office AAMBO.

➤ **Enabling Objective 5.1.2: Develop policies and governance processes to monitor compliance with approved standards and technical guidance**

- Develop policies, governance and management processes and other necessary guidance/directives that enforce compliance with DoD, JIE and Army architecture, and COE guidance to achieve standardization.
- Enforce the use of the Army Application Migration Business Office – PD EC as the single point of coordination for Army application migration to DISA and/or commercial CSPs.
- Leverage Network Capability Set (operational and institutional) oversight and governance bodies and Army Enterprise Network Council (AENC) management processes to synchronize, integrate and govern the Army's enterprise IT portfolio.
- In coordination with the U.S. Army Cyber Command, define organizational roles and responsibilities for assessing risk in, managing, operating and continuously monitoring the network.
- Develop policies, processes and any other necessary guidance/directives needed to standardize and leverage cloud-based infrastructure solutions and services.
- Exercise governance through the AENC General Officer Steering Committee and other appropriate senior leader decision-making bodies to provide oversight of cloud migration plans and activities and enforce compliance with approved cloud architectures.
- Enable an agile development and deployment environment for new and innovative applications, which includes leveraging the breadth of Army science and technology capabilities (e.g., Research, development and Engineering Command).

➤ **Enabling Objective 5.1.3: Develop integrated architectures that define cloud computing capabilities and inform and guide the Army's transition to cloud computing technologies**

- Develop technical and solution architectures to influence/facilitate the delivery and adoption of cloud computing capabilities.
- Establish reference and solution architectures enabling secure operation of cloud computing capabilities.
- Develop and implement Army enterprise service management architecture to standardize service management processes and procedures.

5.2 Instantiate Cloud Computing Capabilities within the Army Network

This imperative aligns to the ANCP LOEs Increase Network Throughput and Ensure Sufficient Computing Infrastructure and Extend Enterprise Service to the Edge.

➤ **Enabling Objective 5.2.1: Increase network throughput and ensure sufficient computing infrastructure**

- Working with DISA, complete the Multiprotocol Label Switching core transport and other modernization upgrades to increase capacity and improve diversity and load balancing.
- Incrementally upgrade installation infrastructure to provide a consistent end-user experience and enable the Installation as a Docking Station [23] initiative.
- Ensure that centralized hosting locations provide sufficient computing infrastructure.

➤ **Enabling Objective 5.2.2: Identify and leverage appropriate cloud service models**

- Adopt appropriate CSPs and/or software solutions, services and platforms without modifications whenever feasible.
- Leverage DoD-approved IaaS service providers for Army-unique systems and applications where owners require total management and control of the operating system.
- Leverage DoD-approved PaaS service providers for Army-unique application hosting to the maximum extent possible to gain efficiency through enterprise license agreements and to reduce potential security vulnerabilities.
- Leverage DoD-approved SaaS provider solutions for identified enterprise services, such as email, messaging, collaboration/web services, Unified Capabilities, etc., to capitalize on economies of scale, improve interoperability, increase collaboration effectiveness and provide a consistent user experience.
- Leverage lessons learned from the IC GovCloud's Discovery SaaS model to improve data visibility and information integration.
- Define a limited set of cloud-based infrastructure packages necessary to support the full range of Army operational and business needs and mission environments.
- Conduct centrally controlled pilots to validate, refine and publish enterprise application migration and development processes and policies.
- Identify standardized cloud-based infrastructure solutions and services that meet Army mission needs.
- Properly categorize applications in accordance with the Risk Management Framework, the DoD CC SRG and the Army Enterprise Cloud Computing Reference Architecture to determine the appropriate government or commercial hosting model.
- Develop a catalog of existing infrastructure, application and data services mapped to functions, missions and business operations to enable re-use.
- Establish processes and business rules for on-demand delivery of services and metering capabilities, including performance and usage monitoring and reporting, to support SLA compliance and utility-based billing.

➤ **Enabling Objective 5.2.3: Integrate secure mobile computing capabilities**

- Establish or leverage Enterprise Mobile Device Management and a Mobile Application Store where authorized end users can retrieve and install approved

mobile applications that support all approved mobile devices accessing services from the cloud.

- Adopt commercially available mobile applications that enable the use of cloud-hosted solutions to the maximum extent possible.
- Develop Army-specific mobile applications that leverage cloud computing and storage capabilities, and consciously reduce and optimize network resource usage.
- Leverage the DoD CIO Cloud Computing Strategy [2] and Army IdAM Reference Architecture [24] for cyber security policies and standards to rapidly mature processes for using commercial cloud and secure mobile computing capabilities while minimizing the potential impact to Army and DoD deployed and contingency forces.
- Evaluate a cloud-enabled “bring your own device” capability to make authoritative information more widely available to the Total Force while reducing overall costs.
- Ensure appropriate implementation and management of Security Technical Implementation Guides and DoD CC SRG controls/protection profiles for management of end points.

5.3 Manage the Modernization and Migration of Applications, Data and Systems

This imperative aligns to the ANCP LOEs Increase Network Throughput, Ensure Sufficient Computing Infrastructure and Extend Enterprise Service to the Edge and Strengthen Network Operations.

➤ Enabling Objective 5.3.1: Maintain the single Army Application Migration Business Office – PD EC within PEO EIS

- Assist system/application owners with modernization and migration requirements, and negotiate and acquire cloud capabilities from approved CSPs.
- Facilitate the transition of user IT services from local implementations to enterprise capabilities to provide a consistent user experience.

➤ Enabling Objective 5.3.2: Modernize applications to conform and operate in a standard, enterprise, cloud-enabled environment

- Ensure that data will be visible, accessible, understandable, trusted and interoperable in accordance with the Army Information Architecture [20].
- Properly categorize applications and data in accordance with the Risk Management Framework and the DoD cloud security model.
- Rationalize and consolidate remaining systems and applications to standardized computing, hosting and storage infrastructure.

➤ Enabling Objective 5.3.3: Ensure that data will be visible, accessible, understandable, trusted and interoperable in accordance with the Army Information Architecture.

- Rationalize associated application data sources to retrieve data elements from defined authoritative data sources to the maximum extent feasible.
- Leverage the DoD data service environment [25] registry to identify and promote the use and reuse of authoritative data sources and standard data services for application development.

- Facilitate transition to publish/subscribe data exchange capabilities that can replace current point-to-point data exchanges.

5.4 Secure and Manage Cloud Operations

This imperative aligns to the ANCP LOEs Enhance Cyber Security Capabilities and Strengthen Network Operations.

➤ **Enabling Objective 5.4.1: Ensuring security and reducing risk**

- Establish the defense-in-depth posture described by the JIE cybersecurity architecture through Joint Regional Security Stacks (JRSS) and the Joint Management System (JMS) to provide boundary and IT infrastructure protection and accommodate active cyber defense measures when appropriate.
- Make access control dynamic by leveraging enterprise IdAM, the Army IdAM Reference Architecture [24] and attribute-based access control capabilities to enforce the principle of least required privilege to determine which services, applications and data an authorized user, on an approved device, can access and for what purposes.
- Centralize security vulnerability and patching management, and ensure standard, approved baselines across the enterprise.
- The cloud construct allows more efficient security management to address vulnerabilities across the Army IT infrastructure.
- Improve overall cybersecurity posture by transferring security vulnerability and patching management of applications and systems to a secure cloud architecture.
- Account for end-to-end security in a cloud environment, including host applications and/or client extensions and data in transit.
- Increase security by enabling an elastic environment where threats can be absorbed, and leverage the Big Data analytic environment that the cloud enables.
- Maintain provenance and integrity of data that have been accessed by users, and leverage security approaches to separate and protect data through virtualization and encryption.
- Fully leverage DoD resources, such as DISA's cloud access point and JIE enterprise perimeter protection.
- Improve effectiveness and enable cyber, computer network defense and network operations.
- Partner with CSPs, FedRAMP and DISA's authorizing official to obtain appropriate Army-level approvals and ensure compliance.
- Follow the mission-focused system categorization security model.
- Capabilities that will be hosted in the cloud will meet RMF requirements.
- Ensure approved encryption of data in transit and while at rest, and the accounting of key management strategies.

➤ **Enabling Objective 5.4.2: Develop standards for acquiring and managing cloud operations**

- Develop CONOPS for operation and management of applications transitioned into enterprise environments.
- Develop standard contractual terms and conditions and service level agreements.

UNCLASSIFIED

- Establish processes and business rules for roles and responsibilities for cybersecurity and continuous monitoring of government and commercial CSPs, to include legal authorities and boundaries, service desk interoperability, end-to-end data management and a clear exit/transition strategy.
- Integrate Army computer network defense service provider functions into CSPs' management frameworks.
- Standardize and automate to the maximum extent possible the system administration processes employed throughout the network.

6. ROLES AND RESPONSIBILITIES

DoD CIO: Develops DoD strategies, policies and guidance, and sets strategic direction for establishing a unified and comprehensive whole-of-government approach to cloud computing. This includes a DoD-wide cloud computing program that harnesses interagency collaboration, cooperation and coordination and promotes the synergistic implementation and integration of cloud computing requirements throughout the department.

DISA: Issues and maintains the minimum cloud computing security requirement guidelines (SRG) and security technical implementation guidance (STIGs) for DoD cloud computing. In addition, DISA provides the DoD cloud access points, reviews FedRAMP authorization packages for CSP compliance with the DoD SRG, grants provisional authorizations and maintains a comprehensive catalog of CSPs authorized for use throughout DoD.

HQDA CIO/G-6: Develops Department of the Army information management strategies, policies and guidance, and sets strategic direction for the network architecture to ensure that operations are conducted in a secure environment. Additionally, the CIO/G-6 oversees implementation of the Army Cloud Computing Strategy through the AENC governance process. This includes the development of cloud computing reference architectures and associated policies, reviewing and approving business case analysis documentation, and ensuring that CSPs have obtained the required cybersecurity approvals and are at an acceptable level of risk to operate within the Army.

U.S. Army Cyber Command (ARCYBER): ARCYBER, serves as the primary Army headquarters responsible for cyberspace operations in support of Joint requirements; serves as the single point of contact for reporting and assessing Army cyberspace incidents, events, and operations in Army networks; and directs all computer network defense service provider measures to include operations within the cloud.

Second U.S. Army: Provides and manages Army network enterprise services and capabilities, including the mandated core enterprise services required by application owners.

Program Executive Office Enterprise Information Systems (PEO EIS): Maintains the Army Application Migration Business Office (AAMBO) as the single focal point for application and system owners throughout the migration process. AAMBO is responsible for assisting system and application owners with defining modernization and migration requirements, determining the most appropriate cloud deployment model, and negotiating and acquiring cloud capabilities from approved CSPs. In the event that certain cloud capabilities required by the Army are not readily available, PEO EIS Product Director, Enterprise Computing (PD EC) will design and implement such capabilities to meet the requirements and architecture of the of the DC/C/GF CE.

Application/System Owners: The command or functional domain that owns the application/system and is responsible for sponsoring and funding an application or system's functionality, which includes modernization, if required, and migration to a CSP. All application/system owners must working directly with AAMBO to acquire cloud services regardless of the deployment model ultimately selected.

7. CHALLENGES AND MITIGATION

Most Army systems and applications have been designed to operate in protected government facilities with dedicated infrastructure. Although moving to cloud-enabling technologies offers significant benefits, challenges remain. The Army must ensure that it does not compromise its missions by trading confidentiality, integrity or availability of data and information in pursuit of the benefits that the cloud may offer. In addition to those challenges identified in the DoD Cloud Computing Strategy [2], Table 3 below lists challenges and mitigation activities that will help the Army achieve the vision described in this document.

Challenges	Mitigation
Managing the evolution of the enterprise cloud environment to enable Army and JIE objectives	<ul style="list-style-type: none"> Participate in and shape DoD Joint governance of cloud-related activities. Establish comprehensive architecture compliance processes to guide implementation and execution of cloud activities.
Achieving visibility and synchronization of all cloud-related planning, resourcing and acquisition activities at the institutional and operational levels	<ul style="list-style-type: none"> Leverage existing decision-making forums to approve/enforce governance and compliance with established processes. Define stakeholder roles and responsibilities to alleviate unnecessary duplication of effort and allocate funding to the most urgent efforts at the appropriate times.
Ensuring that data and applications migrated to cloud services can be discovered, accessed, stored, used and protected among various DoD components and mission partners	<ul style="list-style-type: none"> Develop a plan that identifies an enterprise approach for end-to-end sharing of data, from institutional to operational. Ensure that data and applications migrating to cloud computing environment comply with standards identified in the Army Information Architecture [20] and Army Data Framework [26]. Develop and mature processes for on-boarding and migrating existing applications to the cloud-enabled environment. Implementation of enterprise-wide IdAM.
Maintaining transition momentum during the incremental delivery of cloud-enabled capabilities	<ul style="list-style-type: none"> Capitalize on pilot opportunities to support early adopters of cloud computing capabilities. Enforce the use of the Army Application Migration Business Office.
Ensuring support for application interoperability and data portability between CSPs, and removal of data from infrastructure	<ul style="list-style-type: none"> Negotiate SLAs that ensure portability of applications and data between CSPs. Enforce the use of Army and DoD data standards. Test and evaluate ahead of contracting actions. Preserve Army ability to change vendors in the future. Drive an agnostic solution and avoid platforms or technologies that “lock” customers into a particular product.
Providing cloud services delivery to edge users operating in a DIL environment	<ul style="list-style-type: none"> Maintain the ability to create and process mission-critical data locally while disconnected. Develop and/or adopt deployable Tactical Processing Nodes with cloud-enabling technology and solutions that provide off-line data processing synchronization for mission-critical applications. Establish consistency semantics for reconciling data when full network connectivity is restored.
Ensuring that the security posture is not degraded after issuance of FedRAMP and/or DISA provisional authorization	<ul style="list-style-type: none"> Develop language that is legally enforceable to ensure that the CSP maintains the protection levels the Army requires. Shape and leverage DoD CIO draft contract and SLA terms and conditions.
Multinational / NATO interoperability and collaboration	<ul style="list-style-type: none"> Continue to work with the JIE Technical Synchronization Office on the evolution of the cloud-enabled MPE CONOPS and architectures.

within a cloud-enabled mission partner environment (MPE)	
Ensuring that data classification levels are not compromised due to "aggregation of data"	<ul style="list-style-type: none"> • Ensure that the security level categories for both information and information systems are based upon Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems, [27] and IC ITE data standards.
Rapid deployment of new technologies hindered by current acquisition and accreditation methods	<ul style="list-style-type: none"> • Review and update processes used by the Army to acquire, certify and accredit information technology systems in order to effectively leverage cloud technologies to support the rapid application and adoption of commercially created technologies.
Incident handling	<ul style="list-style-type: none"> • Ensure that incident handling roles and responsibilities are defined in service agreements for PaaS, SaaS and IaaS models.
Data governance	<ul style="list-style-type: none"> • Data Access Standards: Ensure that the application infrastructure interfaces provided in the cloud are generic or that data adaptors at least can be developed so that portability and interoperability of the application are not significantly impacted. • Data Separation: Ensure security protection methods required by the Army to separate data impact levels are in accordance with the Army's Cloud Reference Architecture. • Data Integrity: Employ checksums and replication techniques for data integrity. • Data Regulations: Meet relevant federal and DoD statutes and directives (e.g., those that may prohibit the storage of data outside certain physical boundaries or borders). • Data Disposition: Ensure mechanisms for reliably deleting consumer data on request, as well as providing evidence that the data were deleted. • Data Recovery: Ensure examination of data backup, archiving and recovery.
Security and Reliability	<ul style="list-style-type: none"> • Encryption: Ensure that strong (FIPS 140-2 compliant) encryption is used for web sessions and other network communications sessions; ensure that approved data-at-rest and in-transit encryption standards are provided, to include a key management plan. • Authentication: Ensure the use of authentication tokens or other appropriate form of advanced authentication. • Identity and Access Management: Ensure visibility into authentication and access control mechanisms that the provider infrastructure supports, the tools that are available for consumers to provision authentication information, and the tools to input and maintain authorizations for consumer-users and applications without the intervention of the provider. • Performance Requirements: Benchmark current performance scores for an application and establish key performance score requirements before deploying applications to a provider's site. • Visibility: Ensure that the provider allows visibility into the operating services that affect specific consumer's data or operations on that data, including monitoring system welfare.

Table 4: Challenges moving to a Cloud Environment

8. PATH AHEAD

This strategy and the Army Network Campaign Plan 2020 and Beyond will guide the development and refinement of more detailed implementation plans, which will be the key to executing the Army's vision for cloud computing. By resourcing and implementing the capabilities required in the Army Network Campaign Plan 2020 and Beyond, and the near-term (FY15-16) and mid-term (FY17-21) implementation guidance, the Army will have set the conditions to utilize cloud computing as a means to achieving its 2025 vision.

In order to realize the cloud computing vision, the Army will improve network security and throughput to ensure that sufficient capacity exists for edge users to access and work within the cloud. Simultaneously, the Army will continue rationalization of existing systems, applications and data sources while determining the most appropriate cloud service / deployment models for migration and setting the conditions to improve secure mobile computing capabilities. The Army intends to rapidly capitalize on FedRAMP and DoD-approved government and commercial CSPs to the maximum extent possible. This will reduce sustainment and operating costs and the requirement for cybersecurity and contracting resources, shorten implementation timelines, more effectively keep pace with emerging technologies, and allow the Army to take advantage of the larger economies of scale that typically lower costs.

Additional complementary publications are being developed throughout the Army and include: 1) policy and guidance for commercial cloud; 2) CONOPS for enterprise service management; and 3) CONOPS for the operation and management of applications transitioned to enterprise environments. Finally, the CIO/G-6 has published a series of architecture products, which include the Army Enterprise Cloud Computing Reference Architecture (RA), the End-User Device RA, the Common Operating Environment version 3.0 and the Army Information Architecture. Collectively, these products will serve to inform, guide and constrain the development and/or acquisition of various enabling solutions to ensure that Army solutions are efficient, sustainable and interoperable with the DoD Service components and our mission partners.

9. CONCLUSION

Adopting cloud computing technologies and approaches is one critical component in achieving JIE and LandWarNet 2020 and Beyond objectives, as advances in these technologies potentially offer the flexibility and agility needed to support tailored, scalable operations.

Cloud computing will increase the capabilities and responsiveness of both the generating and operating forces and UAPs globally during Joint operational phases whether preparing to deploy in the installation IT environment, en route or engaged as part of a Joint force in a theater of operations. Cloud infrastructure, people and processes will be central to enabling the JIE. The ability to connect to cloud capabilities assures availability, accessibility and security of Army computing and communications resources, authoritative data sources and information from the enterprise to the tactical edge.

The Army intends to leverage cloud technologies as an essential part of enabling the movement of mission command and business systems applications, services and data across all phases of Joint operations. CIO/G-6 recently released the Army Cloud Computing Reference Architecture, [29] which informs, guides, and constrains how the Army will migrate to and leverage cloud solutions. Additionally, CIO/G-6 is releasing a series of documents to guide the Army's migration of existing and future IT capabilities to a cloud environment. This strategy and associated reference architectures will be updated as needed.

Appendix A References

- [1] U.S. Chief Information Officer Vivek Kundra. *Federal Cloud Computing Strategy*. 8 Feb 2011.
<https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf>
- [2] DoD Chief Information Officer. *Cloud Computing Strategy*. 5 Jul 2012.
<http://www.defense.gov/news/DoDCloudComputingStrategy.pdf>
- [3] Defense Information Systems Agency. *Joint Information Environment Operations Concept of Operations (JIE Operations CONOPS)*. 25 Jan 2013.
- [4] Office of the Army Chief Information Officer. *The Army Network Campaign Plan 2020 and Beyond*. 4 Feb 2015
- [5] Office of the Director of National Intelligence. *Intelligence Community Information Technology Enterprise (IC ITE) Conceptual Architecture, Version 1.1*. 12 Aug 2013.
 [IC CIO website] <http://www.dni.gov/index.php/about/organization/chief-information-officer/ic-cio-enterprise-integration-architecture>
- [6] Under Secretary of the Army. *Migration of Army Enterprise Systems/Applications to Core Data Centers*. 9 Jun 2014.
http://ciog6.army.mil/Portals/1/Policy/2014/USA_Policy_Memo_Application%20Migration%20to_Core_Data_Centers_Jun_9_2014.pdf
- [7] U.S. General Services Administration (GSA). *FedRAMP Concept of Operations (CONOPS), Version 1.0*. 7 Feb 2012. http://www.gsa.gov/graphics/staffoffices/FedRAMP_CONOPS.pdf
- [8] Defense Information Systems Agency milCloud
<http://www.disa.mil/Services/Enterprise-Services/Infrastructure/milCloud>
- [9] Assistant Secretary of the Army (Acquisition, Logistics and Technology). *Common Operating Environment Data Center/Cloud Computing Environment Architecture Compliance, Version 2.0.2*. 1 Jun 2014. <https://www.intelink.gov/go/BIS90fr>
- [10] Office of the Army Chief Information Officer. *Annex B, Definitions and Guidance for the COE to the LandWarNet 2020 and Beyond Enterprise Architecture*.
<http://ciog6.army.mil/Architecture/tabid/146/Default.aspx>
- [11] U.S. Army Mission Command/Cyber. *U.S. Army Cloud-Enabled Network Concept of Operations*. 31 Jul 2014.
- [12] Headquarters, Department of the Army. *Army Doctrine Reference Publication 3-0, Unified Land Operations*. May 2012.
- [13] U.S. Department of Commerce, NIST, Computer Security Division, Information Technology Laboratory. Peter Mell & Timothy Grance. *The NIST Definition of Cloud Computing (SP 800-145), Version 15*. September 2011.
<http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>
- [14] U.S. Chief Information Officer Vivek Kundra. *25 Point Implementation Plan to Reform Federal Information Technology Management*. 9 Dec 2010.
<http://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf>
- [15] National Defense Authorization Act for Fiscal Year 2012, Public Law 112-81, Section 2867. 31 Dec 2011.

- [16] Department of Defense. *Designation of DISA as Defense Enterprise Cloud Service Broker*. 26 Jun 2012. <http://www.defense.gov/news/DISADesignation.pdf>
- [17] Department of Defense. *Risk Management Framework for DoD Information Technology (IT)* (DoDI 8510.01). 12 Mar 2014. http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf
- [18] Defense Information Systems Agency for the Department of Defense. *Cloud Computing Security Requirements Guide, Version 1, Release 1*. 12 Jan 2015. http://iase.disa.mil/cloud_security/Pages/index.aspx
- [19] U.S. Army CIO/G-6. *LandWarNet 2020 and Beyond Enterprise Architecture, Version 2.0*. 30 Jul 2014. <http://ciog6.army.mil/Architecture/tabid/146/Default.aspx>
- [20] U.S. Army CIO/G-6. *Army Information Architecture, Version 4.1*. 5 Jun 2013. [CAC required] <https://www.intelink.gov/go/HbzNmjL>
- [21] Department of Defense Information Network Cloud Computing Services Interoperability and Portability Reference Architecture. <https://software.forge.mil/sf/go/doc58850>
- [22] U.S. Department of Commerce, NIST, Computer Security Division, Information Technology Laboratory. L. Badger, T. Grance, R. Patt-Corner, and J. Voas. *Cloud Computing Synopsis and Recommendations, NIST Special Publication 800-146*. May 2012. <http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf>
- [23] U.S. Army Training and Doctrine Command Installation as a Docking Station (IaaS) Concept of Operations (CONOPS), Version 1.0. 2 Jun 2014.
- [24] Office of the Army Chief Information Officer. *U.S. Army – Identity and Access Management (IdAM) Reference Architecture, Version 3.0*. May 2014. <http://ciog6.army.mil/Architecture/tabid/146/Default.aspx>
- [25] Department of Defense. *Data Services Environment (DSE)*. [application log on] <https://metadata.ces.mil/dse/policy>
- [26] Office of the Army Chief Information Officer, Army Net-Centric Data Strategy Branch. *U.S. Army Enterprise Army Data Framework (ADF): Overview, Version 1.0*. 23 Apr 2012. [CAC required] <https://www.intelink.gov/go/y4iqGSc>
- [27] U.S. Department of Commerce, NIST. *Federal Information Processing Standards Publication 200: Minimum Security Requirements for Federal Information and Information Systems*. March 2006. <http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>
- [28] U.S. Army CIO/G-6. *End User Device Reference Architecture, Version 1.0*. 29 Sep 2014. <http://ciog6.army.mil/Architecture/tabid/146/Default.asp>
- [29] U.S. Army CIO/G-6. *U.S. Army Enterprise Cloud Computing Reference Architecture (Aligned to the DoD Enterprise), Version 1.0*. 29 Sep 2014.
- [30] Training and Doctrine Command. *Pamphlet 525-3-1: The U.S. Army Operating Concept (AOC)*. 7 Oct 2014. <http://www.tradoc.army.mil/tpubs/pams/TP525-3-1.pdf>
- [31] U.S. Department of Commerce, NIST, Computer Security Division, Information Technology Laboratory. Wayne Jansen and Timothy Grance. *Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication 800-144*. December 2011. <http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf>

UNCLASSIFIED

[32] DoD Chief Information Officer. *DoD Cloud Way Forward, Version 1.0*. July 23, 2014. https://disa.deps.mil/ext/cop/iase/_layouts/WordViewer.aspx?id=/ext/cop/iase/Documents/u-fouo_dodcloudwayforward_v1-0_final_0723.docx&DefaultItemOpen=1

[33] Defense Information Systems Agency. *Enabling the Joint Information Environment (JIE – Shaping the Enterprise for the Conflicts of Tomorrow)*. 5 May 2014. <http://www.disa.mil/About/Our-Work/JIE>

[34] DoD Chief Information Officer. *Updated Guidance on the Acquisition and Use of Commercial Cloud Computing*. 15 December 2014.

This page intentionally left blank.

Appendix B Acronyms

ABAC	Attribute-Based Access Controls
ADCCP	Army Data Center Consolidation Plan
ADF	Army Data Framework
ADRP	Army Doctrine Reference Publication
ADS	Authoritative Data Sources
AENC	Army Enterprise Network Council
ANCDS	Army Net-Centric Data Strategy
BYOD	Bring Your Own Device
CC SRG	Cloud Computing Security Requirements Guide
COE	Common Operating Environment
CSP	Cloud Service Provider
DCCE	Data Center/Cloud Computing Environment
DIL	Disconnected, Intermittent or Low Bandwidth
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDIN	Department of Defense Information Network
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Personnel, Leadership & Professional Development, Facilities and Policy
DSE	Data Service Environment
EIS	Enterprise Information Systems
FedRAMP	Federal Risk and Authorization Management Program
FOUO	For Official Use Only
GOSC	General Officer Steering Committee
GSA	General Services Administration
IaaS	Infrastructure as a Service
IAW	In accordance with
IC-ITE	Intelligence Community Information Technology Enterprise
IdAM	Identity and Access Management
IPT	Integrated Process Team

UNCLASSIFIED

IT	Information Technology
JCS	Joint Chiefs of Staff
JIE	Joint Information Environment
JMS	Joint Management System
JRSS	Joint Regional Security Stack
LWN	LandWarNet
MAS	Mobile Application Store
MDEP	Management Decision Evaluation Package
MPLS	Multiprotocol Label Switching
NIST	National Institute of Standards and Technology
O&M	Operation and Maintenance
mPaaS	Platform as a Service
PD EC	Product Director Enterprise Computing
PEG	Program Evaluation Group
PEO	Program Executive Office
PEO EIS	Program Executive Office Enterprise Information Systems
PHI	Protected Health Information
PII	Personally Identifiable Information
POM	Program Objective Memorandum
RA	Reference Architecture
RAM	Random Access Memory
SaaS	Software as a Service
SLA	Service Level Agreement
SSA	Single Security Architecture
TPN	Tactical Processing Node
UAP	Unified Action Partner
UC	Unified Capabilities

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED