U.S. Army Enterprise Cloud Computing Reference Architecture

(Aligned to the DOD Enterprise)

Version 1.0 29 Sep 2014

Executive Summary

In order to improve mission and business effectiveness and achieve operational information technology (IT) efficiencies, the Army is adopting Cloud Computing technologies and approaches. This adoption is one critical component in achieving Joint Information Environment (JIE) and LandWarNet (LWN) 2020 objectives. By transitioning to cloud computing, the Army expects to realize efficiencies in data center operations, application performance, and reduced overall IT costs.

The U.S. Army Enterprise Cloud Computing Reference Architecture (AECCRA) is being developed incrementally to provide guidance for the Army's transition to Cloud Computing. Three versions of the document are anticipated with each version being additive in scope to allow for the evolution and maturity of Cloud Computing technology. The scope of this version of the reference architecture (RA) addresses enterprise-level secure and non-secure fixed Army Enterprise Cloud Computing Environment (AECCE) instantiations implemented in DOD, Federal, Mission Partner or Commercial data centers. The next version will focus on data storage management, as well as application and data migration. Version 3 will address support for the Army Deployed Cloud and interoperability with the Intelligence Community (IC) Cloud.

The technique employed within the RA is the Rules-Based Methodology, which organizes architecture data to align with capabilities, gaps and outcomes derived from the principles, rules, and standards presented within the Department of Defense (DOD) Information Enterprise Architecture (DOD IEA), the JIE, LWN 2020 and Beyond Enterprise Architecture, the Common Operating Environment (COE) and other emerging documents. Documenting information in this fashion allows architecture data to be provided incrementally and provides an effective and timely means of codifying the Army Chief Information Officer's (CIO's) strategy, position and intent in order to solve a specific problem or enable a specific capability.

The intended audience for this RA includes, but is not limited to, HQDA CIO/G-6, Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASA(ALT)), ASA(ALT) Program Executive Officers (PEOs), Office of Business Transformation (OBT), as well as technical and solutions architects and engineers involved in the planning, implementation, execution and maintenance of Army cloud computing capabilities. Other significant stakeholders for this RA include Training and Doctrine Command (TRADOC), Army Cyber Command (ARCYBER), Army Materiel Command (AMC), Forces Command (FORSCOM), Army Service Component Commands (ASCC) and other direct reporting units such as 2nd Army and Intelligence and Security Command (INSCOM).

BLOHM.GARY.W.1228949589

Digitally signed by BLOHM.GARY.W.1228949589
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=BLOHM.GARY.W.1228949589
Date: 2014.09.29 11:19:50 -04'00'

GARY W. BLOHM
Director, Army Enterprise Architecture

Table of Contents

Figures

Tables

1. Introduction

The Army Information Enterprise Architecture (IEA) represents the totality of the LandWarNet architecture, as it supports the Army's warfighting, business, and defense intelligence missions. The IEA consists of three types of architecture: Operational, Systems, and Enterprise Architecture.

The IEA Enterprise Architecture is further sub divided into the LandWarNet Enterprise Architecture, the Network Capability Set (NCS) Reference Architecture, and a set of Enterprise Reference Architectures, all of which the CIO/G-6 develops.

The hierarchy of the IEA Enterprise Architecture, and the context in which it fits, is shown in Figure 1.

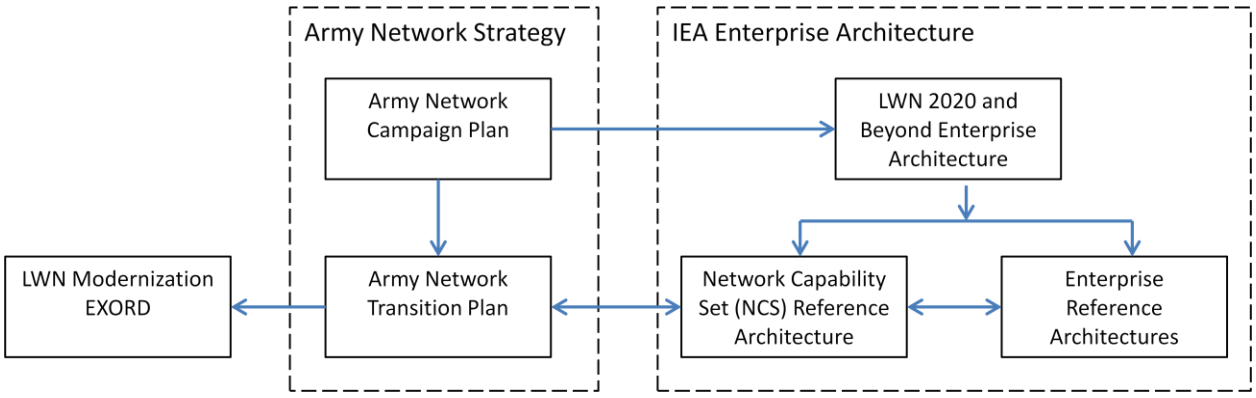

Figure 1: Hierarchy of IEA Enterprise Architecture Documents

The overall objective of this set of documents is to provide the architecture guidance and direction including technical guidance, principles, rules, policy, constraints, forecasts, standards, implementation conventions, and criteria required for LandWarNet to achieve the vision in the Army Network Strategy. Each of these documents has a unique role in the IEA by providing specific architecture-related information, as described below.

- LandWarNet 2020 and Beyond Enterprise Architecture – Captures all CIO/G-6 architecture guidance and direction at the level of detail needed to support the evaluation of potential IT investments and architecture options for their alignment with the Army Network Strategy.
- Network Capability Set (NCS) Reference Architecture – Sets the architecture guidance that drives the design of the future NCS for each fiscal year. It is the architecture roadmap to understand how LandWarNet will transition from its current state to its future state.
- Enterprise Reference Architectures – Aids in the resolution of specific recurring problems and explains context, goals, purpose, and the problems being solved.

The Army Enterprise Cloud Computing Reference Architecture (AECCRA) is a specific instance of an Enterprise Reference Architecture. It provides overarching guidance to support Army efforts to achieve Federal and DOD mandates to transition to cloud computing. This reference architecture shares dependencies with other enterprise reference architectures and successful delivery of the capabilities described herein requires successful delivery of capabilities discussed in the other enterprise reference architectures as components of Network Capability Sets.

1.1 Background

To improve mission and business effectiveness and achieve operational IT efficiencies, the DOD and Army are transitioning to cloud computing technologies. Adopting cloud computing technologies and approaches is one critical component in achieving Joint Information Environment (JIE) and LandWarNet (LWN) 2020 objectives, as advances in these technologies potentially offer the flexibility and agility needed to support tailored, scalable operations.

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 Joint Operations phases. Accordingly, CIO/G-6 is releasing a series of documents to guide the Army's migration of existing and future IT capabilities to a cloud computing environment.

This document is the first of three versions:

- Version 1 is the initial document release of a common set of Army guidelines and requirements for instantiating an AECCE that include Information, Data and Services Management; Operation and Defense; and Governance and Monitoring. This version directly supports efforts of the Army Data Center Consolidation Program (ADCCP) and Program Executive Office Enterprise Information Systems (PEO EIS) to consolidate data center capabilities and deliver materiel solutions that support the Army's transition to cloud computing.
- Version 2 will address data storage management within the AECCE and detailed modernization of applications and data migration process.
- Version 3 will address interoperability with Intelligence Community Information Technology Enterprise (IC ITE).[1] Interoperability reflects AECCE interaction with the IC Cloud to leverage intelligence capabilities in support of Army missions. In addition, this version will address the Deployed Cloud, which includes support of Disconnected, Intermittent, Low Bandwidth (DIL) communications; Local Monitoring and Management; and Data Staging and Forwarding.

Each version is additive, allowing cloud technology to mature and for implementation patterns to evolve, leading to a complete document at version 3.

[1] IC IT Enterprise Fact Sheet, Defense National Intelligence, CIO

Other cloud-enabling capabilities are addressed in separate RAs, such as the following:

- Army Information Architecture
- Identity and Access Management (IdAM)
- Network Operations (NetOps)
- Network Security
- Thin/Zero Client
- Unified Capabilities (UC)

For more information on these and other emerging RAs, please visit: http://ciog6.army.mil/Architecture/tabid/146/Default.aspx/.

1.2 Overview

Historically, the Department of Defense (DOD) has developed and deployed Information Technology (IT) applications, systems and data in a stove-piped manner resulting in increased costs, decreased interoperability and portability, a larger deployment footprint, and tremendous complexity in managing configuration. Additionally, outdated business processes have delayed technology insertion and alignment with commercial innovation. This situation has replicated across the DOD environment leading to unacceptable IT costs and complexity. Declines in budget and force structure combined with expanding operational needs are compelling the DOD to overhaul its IT environment and strategy.

In 2012, the DOD Chief Information Officer (CIO) articulated its intent to transition to cloud computing capabilities via the DOD Cloud Computing Strategy.[2] To reinforce this objective, DOD CIO released subsequent guidance, memoranda and directives aimed at consolidating and standardizing applications and data and shifting IT modernization toward cloud computing capabilities.

So, what is cloud computing? The National Institute of Standards and Technology (NIST) in Special Publication (SP) 800-145 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."[3] This model is composed of five essential characteristics:

- On-demand Self service
- Broad Network Access
- Resource Pooling
- Rapid Elasticity
- Measured Service.

It enables three service models:

[2] DoD Cloud Computing Strategy, 9 January 2012
[3] National Institute of Standards and Technology Special Publication 800-145, September 2011

- Software as a Service (SaaS),
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Lastly, the cloud computing model supports four deployment models:

- Private Cloud,
- Community Cloud
- Public Cloud
- Hybrid Cloud

For Army purposes, Cloud Computing entails the hosting of applications, data and services on standardized, modular computing, storage and network capabilities. These capabilities are located in enterprise-managed Army, DISA, Joint, Mission Partner or commercial cloud service provider (CSP) facilities. These facilities will support metered usage of dynamically provisioned and released capabilities to authorized users on approved devices from any location at any time. While it is the intent of the Army to maximize delivery of capabilities consistent with the NIST definition, early adoption efforts indicate that legal and security restrictions may limit the extent to which the NIST definition can be achieved.

In support of Federal and DOD guidance and in parallel to the development of the AECCRA the Army CIO/G-6 is developing the Army Cloud Computing Strategy. The purpose of that document is to establish and communicate the Army's vision and strategy for transitioning to a Cloud Computing environment, to include describing the path forward to realize the objectives of the Army and DoD leadership to reduce the costs associated with IT operations and maintenance while improving the agility of deployment and the security posture of Army applications on the network.

The path forward described in the Army Cloud Computing Strategy is further articulated in this document, which leverages guidance found in the DOD Reference Architecture Description[4] and uses a Rules-Based Architecture (RBA) approach. Using an RBA, specific functional areas needing principles, baseline rules and desired outcomes can be documented. The collection of rules helps inform, guide and bind the design and implementation of a specific IT initiative or enterprise capability. Rules supporting enterprise guiding principles are developed from existing architectural data, strategic objectives and senior leader guidance and are further described (as required) to clearly articulate the intent, purpose, and use of the rule.

1.3 Purpose

Building upon the Army Cloud Computing Strategy, this rules-based architecture provides enterprise-level technical direction guiding the design, development, procurement and fielding of cloud capabilities in support of Army mission needs. The objectives of this document are as follows:

[4] OASD/NII Reference Architecture Description, June 2010

- Describe the elements and interactions of the Army Enterprise Cloud Computing Environment (AECCE)
- Inform activities associated with the migration of existing applications and data
- Foster improved security and controlled access to applications and data
- Facilitate governance process restructuring to support the transition to cloud computing in alignment with JIE and Army Common Operating Environment standards

Through achievement of these objectives, acquisition organizations will provide initial cloud computing capabilities that support early migrations and provide lesson learned for further, more rapid and seamless transitions to cloud computing technologies.

1.4 Scope

The scope of this version of the reference architecture (RA) is enterprise-level secure and non-secure fixed AECCE instantiations implemented in DOD, Federal, Mission Partner or Commercial data centers.

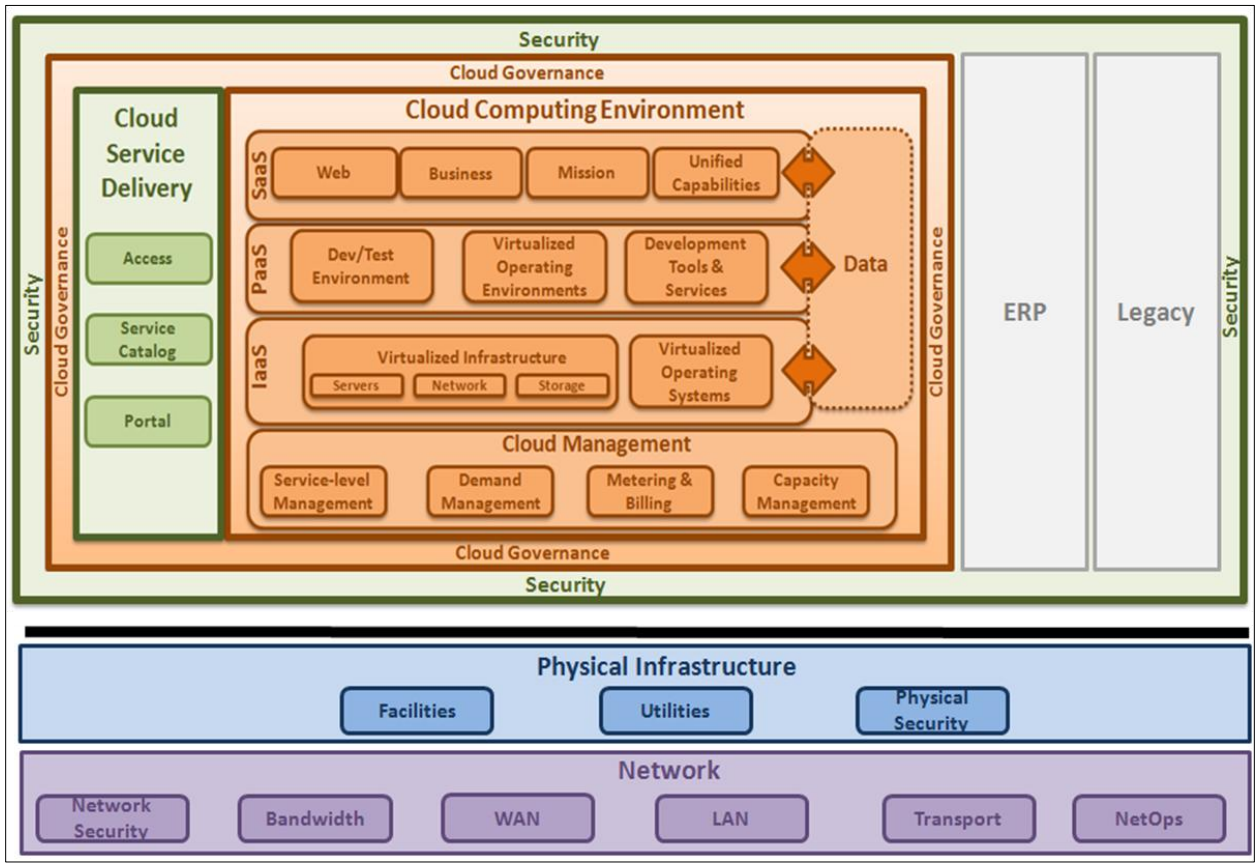

Figure 2: AECCRA In Context Diagram

Figure 2 provides a graphical depiction of the AECCE. This RA will address the elements above the Physical Infrastructure and the Network. It does not address physical security and associated utilities for an installation or a data center facility (e.g., structural, electrical, mechanical, telecommunications or climate control). It is

envisioned that DOD and non-DOD Cloud Service Providers (CSPs) engaged in support of the Army will provide the capabilities within the solid green boundary as described by the principles and rules in this document and negotiated with the consumers of the capabilities.

Initial instantiations of the AECCE will occur in Defense Information Systems Agency (DISA) Defense Enterprise Computing Centers (DECC) that are evolving to become Core Data Centers in accordance with DOD Core Data Center RA[5] and Commercial facilities that are Federal Risk and Authorization Management Program (FedRAMP) compliant[6] and comply with additional security guidelines identified by the DOD Enterprise Cloud Service Broker.[7]

As applications are evaluated for migration preparedness, it will be determined that some are ready to run in a cloud environment, others may need to be modernized, and others still may not become migration ready. The diagram above identifies infrastructure to accommodate each of these situations and represents an interim AECCE that is acquired to support data center consolidation and the cloud transition between now and the end of fiscal year 18, which is the timeframe in which all enterprise applications should reside in Core Data Centers.[8]

1.5 Intended Audience

The intended audience for this RA includes, but is not limited to:

- HQDA CIO/G-6
- Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASA(ALT))
- ASA(ALT) Program Executive Offices (PEOs)
- Office of Business Transformation (OBT)
- Technical and solutions architects and engineers involved in the planning, implementation, execution and maintenance of Army cloud computing capabilities.

Other stakeholders that will influence and may be influenced by this RA include:

- Other HQDA Staff elements
- Training and Doctrine Command (TRADOC)
- Army Cyber Command (ARCYBER)
- Army Materiel Command (AMC)
- Forces Command (FORSCOM)
- Army Service Component Commands (ASCC)

[5] Director, Architecture & Interoperability, Office of the DOD Chief Information Officer, Core Data Center Reference Architecture, Version 1.01, February 5, 2013
[6] FedRAMP Compliant Cloud Systems, http://cloud.cio.gov/fedramp/cloud-systems
[7] DOD Enterprise Cloud Service Broker, http://www.disa.mil/Services/DoD-Cloud-Broker
[8] DOD "Joint Information Environment: Continental United States Core Data Centers and Application and System Migration" 11 Jul 2013

- Other direct reporting units such as 2nd Army and Intelligence and Security Command (INSCOM)

Architects will use the content of the Army Enterprise Cloud Computing Reference Architecture (AECCRA) to develop Mission Area, Component, and solution architectures able to drive JIE-conformant solutions. Investment decision makers use the descriptions of capabilities as a baseline to project and spend funds. Capability developers and managers use capability descriptions to design solutions and then measure their progress toward achieving the desired end state.

1.6 Document Structure

An Army Enterprise RA provides information, guidance and direction that is applicable across the Army. This information, guidance and direction are provided in the following sections:

- **Section 2:** Objective State
  - CV-2a Capability Taxonomy: AEN Portfolio mapping to the DOD/JIE Capabilities
  - CV-2b Capability Taxonomy: AECCE Mapping to AEN Domains
- **Section 3:** Guiding Principles and Rules
- **Appendix A:** StdV-1 Standards
- **Appendix B:** AV-2 Vocabulary (Integrated Dictionary)
- **Appendix C:** Acronyms
- **Appendix D:** References

1.7 Assumptions and Architectural Considerations

Cloud computing is enabled through the synchronization, integration and interoperability of a number of other capabilities. Accordingly, several high-level assumptions are required:

- Delivery of the AECCE has the full support and cooperation of all Army senior leaders, Soldiers and civilians.
- Army Enterprise cloud computing end state is achieved through the iterative delivery of capabilities in conjunction with Network Capability Sets.
- AECCRA will be used to inform and shape solution architectures and implementation plans including technical and engineering specifications.
- Army cloud computing solution architects and developers will use this RA as enterprise guidance for standardizing systems/applications, platforms and data migration into the cloud computing environment.
- Reliable, high bandwidth communication transport links implementing Multiprotocol Label Switching (MPLS) will be available. These links will provide

adequate bandwidth to each installation to support current demand with enough expandable capacity to meet the cloud computing requirements.

- All instantiations of the AECCE will adhere to standards and technical profiles described in the current approved version of the Common Operating Environment.

2. Objective State

Cloud technologies and solutions will provide Army users with access to data and applications over the network from centrally managed enterprise computing and storage locations while enabling, as required, local cloud deployments to support critical operational needs. Figure 3 depicts how the Army will leverage known and evolving capabilities to deliver its concept of a seamless cloud capability integrated within the LWN framework by 2020.

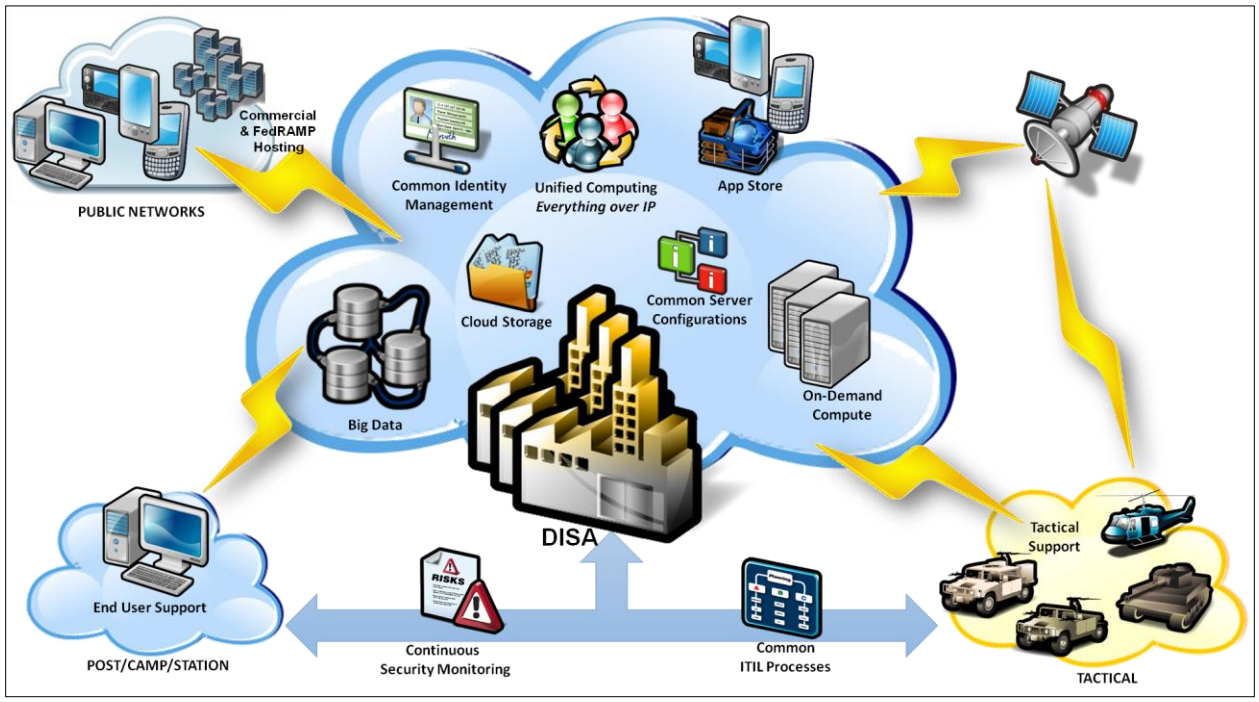

Figure 3: Objective Seamless Cloud Capability

2.1 End-State Vision

By 2020, the Army will maintain strategic and tactical advantage over its adversaries through information dominance by fully leveraging a global mix of government and commercial cloud service providers that support Total Force requirements for quality of service and provide authorized users access to required data elements anywhere, on any device, in any environment. Moreover, these data elements will be customizable to the desired format of Mission Commanders, Senior Leaders, decision makers and other authorized mission partners.

Cloud computing technologies will change how the Army organizes, trains, supports and deploys its formations enabling immediate connectivity to the capabilities and data

necessary to accomplish missions. The AECCE will enable real-time, secure, direct connectivity and data sharing with other DOD Components/Services, Federal Agencies, as well as Joint and commercial partners.

Figure 4 depicts the various cloud environments to be leveraged in the end state. This end state includes support for multi-security level transport of data, appropriate cross-domain solution implementation and the deployment of tools and access to support enterprise-level control and management of a completely federated cloud computing environment. In this federated cloud computing environment, the Army, through negotiated agreements, will leverage services that exist in the Intel Cloud to meet Army Cloud Computing requirements. As well, services will be acquired from the commercial cloud from approved CSPs to host Army applications and data. These services will be managed by Service Level Agreements that will include, but not limited to the topics of CSP connections to DOD networks, appropriate segregation of data, and support for monitoring by DOD Enterprise Operations Centers. The Army will maintain capabilities within Installation Processing Nodes to support local services, local data storage, and support tactical applications in the institutional environment. As units deploy, they will be able to detach infrastructure that supports a Deployed Cloud environment. As transport links are installed, the deployed cloud will reconnect to the Enterprise Cloud to update its data stores.

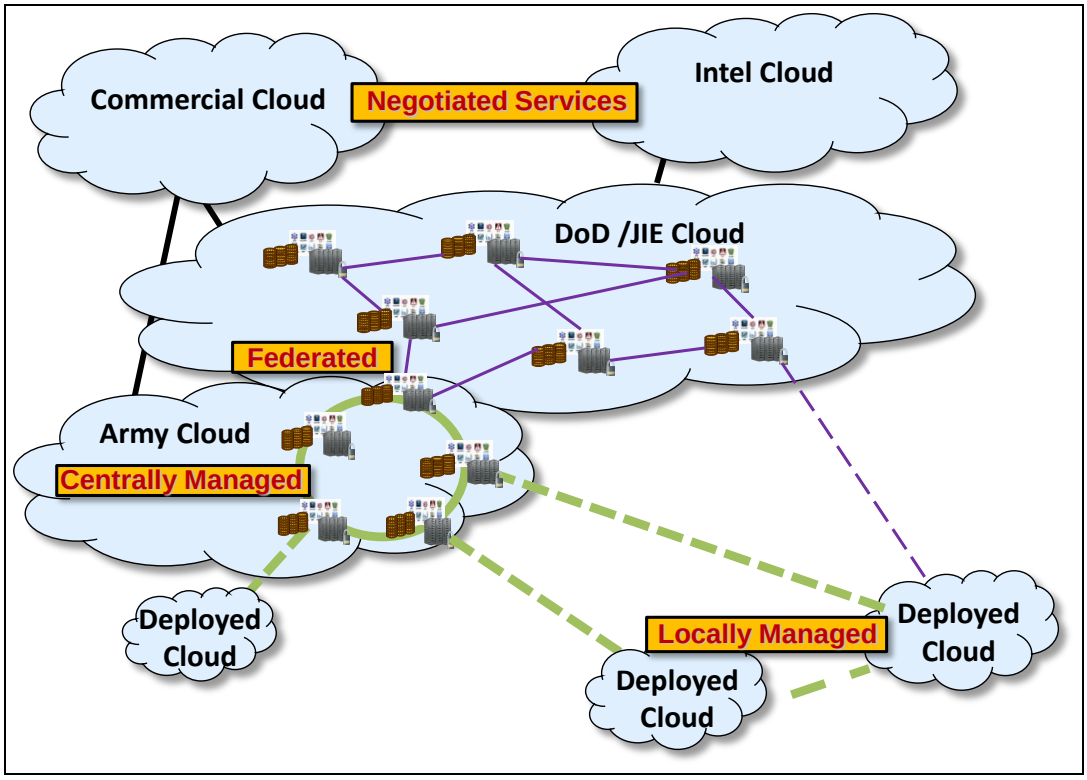

Figure 4: End-State Cloud Computing

2.2 Alignment with Joint, DOD Information Enterprise Architecture (IEA) and Army Enterprise Network (AEN) Portfolio

The focus of this RA is to describe the AECCE. It is aligned with the DOD IEA/JIE and the AEN Portfolio Domains.

The JIE is envisioned as a secure environment comprised of shared information technology infrastructure, enterprise services and cybersecurity architecture to achieve full spectrum superiority, improved mission effectiveness, increased security and the realization of IT efficiencies. Operation and management of JIE is in accordance with the Unified Command Plan, using enforceable standards, specifications and common tactics, techniques and procedures, as described in DoD IEA v2.0 (http://dodcio.defense.gov/Home/Initiatives/DIEA.aspx). The JIE has three major capabilities that are divided into sub-capabilities:

- End User Capabilities: Connect, Access, Share
- Enable Capabilities: Operate, Defend
- Users & Operations Requirement (Govern): Processes, Policy, Compliance

The Army's framework for managing network modernization is the Army Enterprise Network (AEN) portfolio, which manages the Net-Centric (6.0) Joint Capability Areas (JCAs). The portfolio is comprised of three AEN Domains - Network Capacity, Enterprise Services and Network Operations and Security. Each domain is further divided into capabilities:

- **Network Capacity Domain (NCD)**: The NCD portfolio includes the physical infrastructure necessary for all services and information based activities to traverse the network. The portfolio encompasses the foundational infrastructure upon which the Enterprise Services and Network Operations & Security solutions reside. Capabilities within this domain include – Information Transport and Computing Services.
- **Enterprise Services Domain (ESD)**: This portfolio oversees delivery of an easy-to-use, integrated suite of globally available, adaptable solutions that seamlessly supports the Total Force while working with Unified Action Partners (UAPs). These services, both user-facing and enabling, provide the Total Force awareness of and access to information. Capabilities within this domain include - Core Enterprise Services and Position, Navigation & Timing.
- **Network Operations & Security Domain (NSD)**: The NSD is responsible for providing a secure, seamless and continuous network environment with protected critical data and information for the Total Force and UAPs. To meet this objective, NSD will provide capabilities that will improve the Army's ability to protect, detect, respond, restore, and manage information and systems. NSD will also pursue capabilities that support the management of underlying physical assets that provide end user services for a continuous network environment. Capabilities within this domain include - Net Management and Information Assurance/Cybersecurity.

The alignment between DOD/JIE and AEN Domains is depicted in Figure 5. This is a first level of mapping to identify the capabilities associated with the AECCE. It is

provided to support the crosswalk from delivered capabilities back to the DOD/JIE objectives from which they are derived.

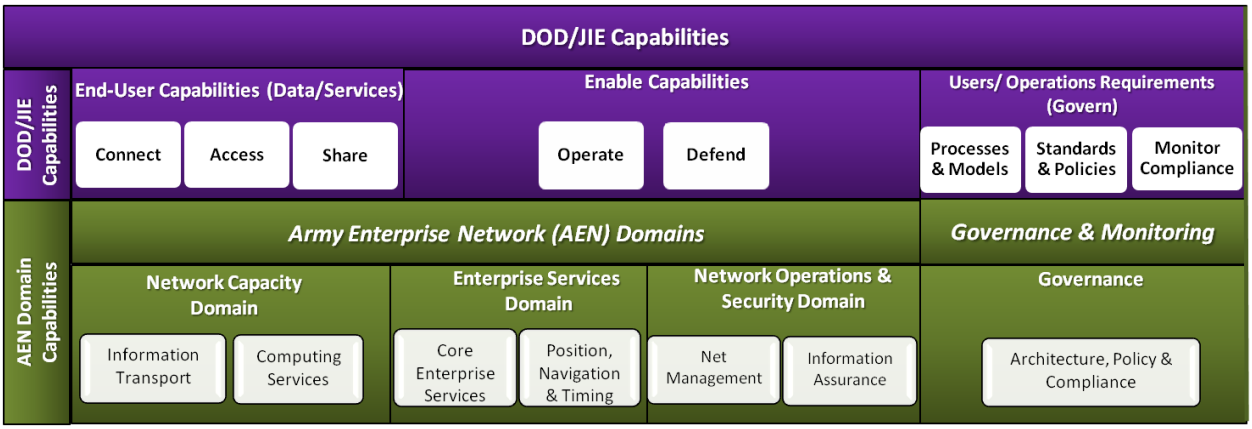

Figure 5: CV-2a Capability Taxonomy: AEN mapping to the DOD/JIE Capabilities

The second level of mapping, as depicted in Figure 6, pertains to cloud-specific capabilities aligned with AEN Domains. Four Army cloud computing capabilities are aligned to the AEN Domains in this RA: (1) Operational AECCE; (2) AECCE Information, Data and Services Management; (3) Operate and Defend the AECCE; and (4) Govern and Monitor AECCE.

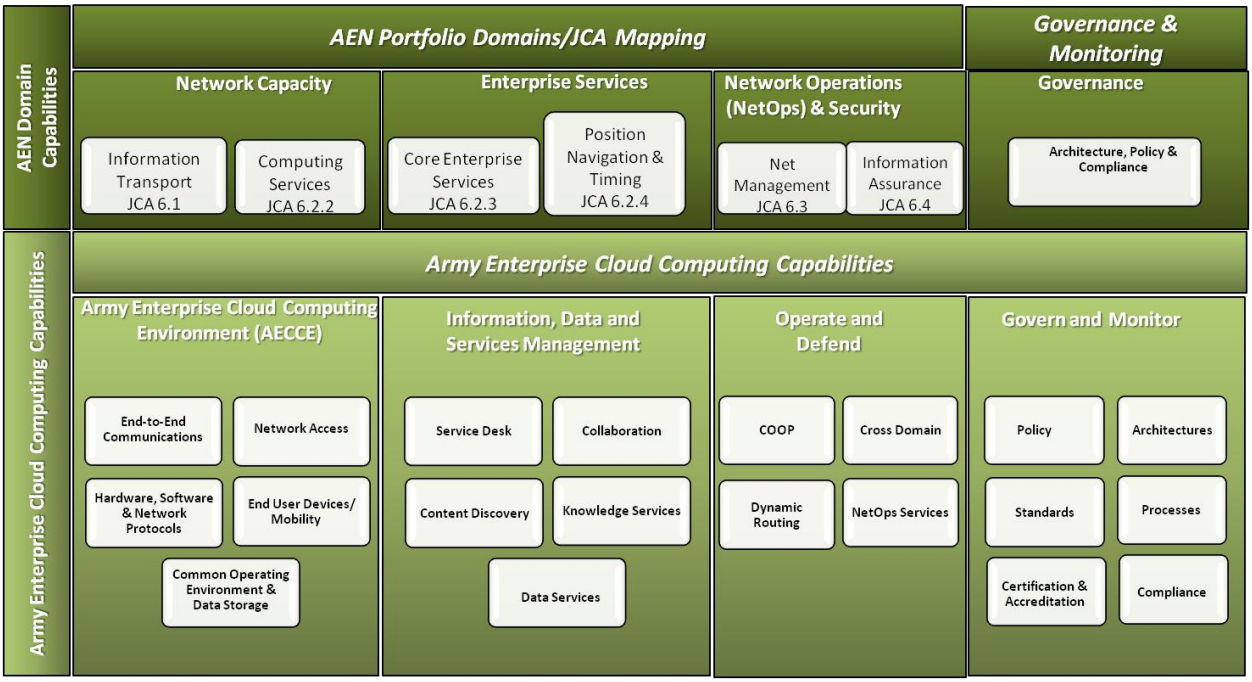

Figure 6: CV-2b Capability Taxonomy: AECCE Mapping to AEN Domains

3. Principles and Rules

RA principles are enduring guidelines that describe how the Army cloud computing environment will fulfill its mission. They express the intent of the capability and fundamental values to be achieved within the Army cloud computing environment. These principles inform and support the Army's cloud computing goals, which are indicated in the emerging Army Cloud Computing Strategy. Business rules are definitive statements that provide design tenets and also constrain the implementation of principles and associated policies, as well as acquisition guidance.

The Interpretive/Bridge Table (1) summarizes the relationships between Figures 5 and 6, presented in section 2. This table sets the framework for the capability mappings to principles and business rules listed in Tables 2 through 11.

DOD/JIE Capabilities	AEN Domain Capabilities		Cloud Computing Capabilities	PR/BR Tables
	Domain Name	Capability		
Connect Access Share	Network Capacity	Information Transport Computing Services	Operational AECCE	Tables 2-3
Operate	Enterprise Services	Core Enterprise Services Position, Navigation and Timing	AECCE Information, Data and Services Management	Tables 4-6
Defend	Network Operations & Security	Net Management Information Assurance	Operate and Defend the AECCE	Tables 7-8
Processes & Models Standards & Policy Monitoring Compliance	Govern	Policy & Guidance	Govern and Monitor AECCE	Tables 9-11

Table 1 - Interpretive/Bridge Table

The following AECCE capabilities are mapped to high-level JIE Capabilities and IEA principles (PRs)/business rules (BRs). These mappings will be updated in alignment with newer versions of the DOD IEA and DOD Data Center RAs when the newer versions become available. Additional detail on the planned capabilities of the COE based AECCE can be found in the ASA(ALT) COE Data Center/Cloud Computing Environment Architecture Addendum; v2.0.2, 1 June 2014, as well as the ASA(ALT) COE Data Center/Cloud Computing Environment Architecture Compliance document, v2.0.2, 1 June 2014.

What follows in this section of the document is a common set of principles, rules and standards that an AECCE instantiation must satisfy. The tables that follow include principles and business rules derived from Federal, DOD and Army Strategy, Guidance, and Enterprise Architecture documentation. Principles are labeled with ***CCEX.Y*** and Army business rules with ***CCEX.Y.Z***. CCE represents Cloud Computing Environment. X represents the document version number, Y represents an Army principle, and Z represents a rule associated with a principle.

3.1 Operational AECCE

The AECCE capability consists of computing infrastructure, computing storage, HW/SW Protocols, End-User Devices (EUD), Network (NW) Access and Command and Control (C2). Benefits derived from the AECCE are: improvement of our network's efficiency by consolidating infrastructure & enterprise licenses; eliminating redundant capabilities, operations and services to allow us to increase our focus on the most promising new systems and technologies; optimizing operations and training at installations and while deployed. The AECCE is a component of the LandWarNet 2020 & Beyond plan and leverages the capacity, security and enterprise services delivered by LandWarNet. The operational AECCE will be a hybrid cloud instantiated as DOD community and service private clouds in DOD and non-DOD facilities.

CCE1.1: Approved DOD and non-DOD CSPs are available to provide computing infrastructure able to provide secure, dynamic, computing platform-agnostic and location-independent application hosting and data storage in support of the AECCE
CCE1.1.1: Army Acquisition community will acquire capabilities to support the cloud service models (IaaS, PaaS, SaaS) in order to provide environments for application and data migration and provide interim environments for enterprise hosting of non-cloud ready ERP and legacy applications.
CCE1.1.2: Non-DOD CSP facilities hosting AECCE data must be subject only to US legal jurisdiction.
CCE1.1.3: Cloud Service Providers (CSP) (DOD and Non-DOD) shall be responsible for the cloud infrastructure (operating system and below) to include backups, system maintenance, patch management, power management, hardware and operating environment software refresh and Continuity of Operation Program (COOP); physical infrastructure to include security, heating, ventilation and air conditioning (HVAC); and network connectivity in accordance with (IAW) service level agreements (SLA), Memorandums of Agreement (MOA) and Contract Terms and Clauses.
CCE1.2: Infrastructure hosting the AECCE is scalable, changeable, deployable, and rapidly manageable while anticipating the effects of the unexpected user. (DOD IEA, V2.0, Vol. II, B-4, SIP 03)
CCE1.2.1: AECCE will support the dynamic provisioning of computing resources throughout the federated cloud, where authorized by pre-approved rules or approved by authorized consumers, as needed within approved funding threshold limits.
CCE1.3: Infrastructure supporting the AECCE supports full Internet Protocol (IP) version 6 convergence of traffic (voice, video, and data) on a single network, within a security domain.
CCE1.3.1: The AECCE shall support IPv6 compliance and retain IPv4 capability for support of legacy applications/systems still using that standard.
CCE1.4: The AECCE leverages transport capabilities of the LandWarNet and commercial providers to provide reliable end user access to required applications/data with a contingency plan for a “disconnected mode" and for continued local processing during network outages (COOP).
CCE1.4.1: CSPs will comply with COOP guidelines and requirements to avoid or minimize disruption of the operations IAW current AR 500-3 U.S. Army Continuity of Operations Program Policy and Planning.
CCE1.4.2: CSPs will develop a detailed COOP, which includes customer identified Mission Essential Functions (MEFs) for disaster recovery along with backup and recovery for the scheduled data/databases, application, servers, storage devices and web services IAW SLA.

Table 2 - Computing and Storage Infrastructure

CCE1.5: The AECCE supports computing services request from all enterprise approved software applications, as well as authorized end-users, including those changing their points of attachment among alternate operational and network domains and/or communities of interest. (DOD IEA, V2.0, Vol. II, B-4, SIP 02).
CCE1.5.1: AECCE will enable authorized user access to the applications, data and information from anywhere, anytime from any Army approved end-user device.
CCE1.5.2: End-users will have the same user experience (i.e. look, feel, content, utility, etc.) regardless of location or end-user device, to the extent possible.
CCE1.5.3: AECCE will tailor the view presented to each user based on their role(s), the trust level of the network enclave, and the IT capabilities provided to their organization.
CCE1.5.4: All IT components within the AECCE will be capable of being configured remotely.

Table 3 - End-User Connectivity

3.1.1 Assumptions

- To the extent feasible, cloud computing solutions are COTS hardware and software vendor neutral.
- Information consumers do not have physical control or real-time visibility into all cloud activities.
- Cloud implementation with COOP and Disaster Recovery infrastructure requirements will be equal or better than current capabilities.
- Virtualized applications, systems and databases will improve continuity of operations and disaster recovery through the ability to change datacenter operating locations electronically.

3.1.2 Risks

- Latency due to Enterprise (connectivity, bandwidth, application …etc.) issues.
- Degradation of expected user experience.
- Transition to IPv6 can interrupt operations due to its non-compatibility and lack of interoperability with current IPv4 networks.
- COOP plans will be complicated requiring synchronization of the continuity of operations across applications, IP protocols, security domains, software applications and with software applications running other software applications in the background
- Without network connectivity, users will have limited or no access to applications and data
- Multi-layered organizational boundaries will potentially impact response times, creating delays in action on operational request for adds, changes, and break/fix activities due to the complexity of hands-off, formalized channels of communication and differing priorities.
- Different/more complex IA guidelines to follow.
- Management construct may be radically different from what is familiar.
- Lack of definition and strategy for implementing a utility billing model.

3.2 AECCE Information, Data and Services Management

Aligning with DOD requirements to transition to an Enterprise Cloud may require modifications to the design and implementation of applications and moving data from installations to the DOD cloud computing environment. Army users will access cloud-based solutions and enterprise capabilities that are available through a browser from anyplace, anywhere and anytime, such as: Enterprise Email, Enterprise Portal, Enterprise Web Hosting, Enterprise Storage and Unified Capabilities.

CCE1.6: AECCE data assets, services, and applications are visible, accessible, understandable, and trusted to authorized (including unanticipated) users. Unanticipated users may include Joint, interagency, intergovernmental, and multinational partners. Access granted may be limited by law, policy, security classification, or operational necessity.
CCE1.6.1: The AECCE will provide a mechanism for end-users to discover the IT services available to them, and the conditions of their use.
CCE1.6.2: AECCE authoritative data assets and capabilities shall be advertised in a manner that enables them to be searchable from an enterprise discovery solution. (DOD IEA, V2.0, Vol. II, B-2)
CCE1.6.3: Mission or business functions hosted in the AECCE will be made available to authorized users as a network-based service with a published, well-defined interface. (DOD IEA, V2.0, Vol. II, B-2)
CCE1.6.4: All AECCE information services and applications must uniquely and persistently digitally identify and authenticate users and devices. These services, applications, and networks shall enforce authorized access to information and other services or devices according to specified access control rules and quality of protection requirements for all individuals, organizations, COIs, automated services, and devices. (DOD IEA, V2.0, Vol. II, B-4)
CCE1.6.5: AECCE will provide timely access to critical data, services, and applications from any access point upon authentication of the user and their end-user device. (DOD IEA, V2.0, Vol. II, B-7)
CCE1.7: Army leveraged CSPs are capable of supporting DOD and Army specific services.
CCE1.7.1: Facilities hosting the AECCE shall be capable of enabling Army specific local services per SLAs.
CCE1.8: COE compliant software development environments are enabled in AECCE instantiations.
CCE1.8.1: AECCE will provide a set of application development tools (programming languages, run-time environments, test environment) to facilitate high-quality, scalable application development/deployment.
CCE1.8.2: All applications available from the AECCE will be developed, tested and integrated in software development environments compliant with the currently approved COE. AECCE hosting of applications not developed in COE compliant environments must be approved by CIO/G-6 (as may be the case for COTS software).
CCE1.8.3: All applications hosted in the AECCE will be evaluated and where cost effective modernized to operate in a cloud-enabled environment. Evaluation of applications shall be conducted in accordance with Enclosure 1: Application Migration Process Overview and Enclosure 2: System/Application Modernization Checklist of the Under Secretary of the Army Memorandum, Subject: Migration of Army Enterprise Systems/Applications to Core Data Centers, dated 9 Jun 2014.

Table 4 - Core Enterprise Services

CCE1.9: All information to be hosted in the AECCE will be assessed for impact if the information confidentiality or integrity is compromised and assigned an impact level (1-6) based on definitions provided in the DOD Cloud Way Forward and DOD Enterprise Cloud Service Broker (ECSB) Cloud Security Model (CSM): • Impact Level 1: Unclassified-Public, approved for public release • Impact Level 2: Unclassified-Limited Access, approved for public release but is intended for a limited public audience • Impact Level 3: Non-National Security System (non-NSS) Controlled Unclassified Information (CUI) e.g., training systems • Impact Level 4: Non-NSS CUI e.g., HR systems • Impact Level 5: NSS CUI e.g., email systems • Impact Level 6: Classified information up to and including SECRET e.g., C2 systems DOD Cloud Way Forward: https://software.forge.mil/sf/docman/do/listDocuments/projects.dodcloud/docman.root.dod_cloud_mildep_js_disa_cio_wg.13_august_2014 DOD ECSB CSM: http://iase.disa.mil/cloud_security/Pages/index.aspx
CCE1.9.1: Army cloud users will identify the DOD ECSB impact level (1-6) of their application, data, or system, and ensure the CSP enables appropriate information separation in their hosting environment.
CCE1.10: Non-DOD CSPs are capable of providing appropriate data-separation in accordance with guidelines provided in the DOD Cloud Way Forward.
CCE1.10.1: Non-DOD CSPs may implement virtual or physical separation between DOD and Non-DOD tenants when hosting Army impact level 1 and 2 information.
CCE1.10.2: Non-DOD CSPs must implement physical separation between DOD and Non-DOD tenants when hosting Army impact levels 3 - 5 information.
CCE1.11: Owners of information and applications/services must establish and refine access policies to allow "need to know" access to appropriate user, even the rare or unanticipated user whose role and assigned mission require access.
CCE1.11.1: AECCE will provide technologies in support of archiving, retrieving, and reliably deleting data.
CCE1.11.2: AECCE will use existing enterprise data, services, and end-user interfaces whenever possible, practical, and appropriate, instead of re-creating those assets. (DOD IEA, V2.0, Vol. II, B-2, DSDR 11)
CCE1.11.3: AECCE will use metadata containing access control and quality of protection attributes that is strongly bound to or associated with information assets to make access decisions. (DOD IEA, V2.0, Vol. II, B-4, SAR 08)
CCE1.11.4: AECCE will include a mechanism for end-users to search for available data assets, and the data models or schema that define them. This mechanism should support the DOD Discovery Metadata Specification (DDMS) http://metadata.ces.mil/dse/irs/DDMS/.
CCE1.11.5: Data in the AECCE shall be decoupled from the applications and systems that use them to facilitate easier discovery, use and protection.
CCE1.11.6: Application owners and developers will minimize redundant data entry and identify approved, authoritative data sources to support application and system data requirements.

Table 5 - Information and Data Management

CCE1.12: AECCE facilitates remote application and data management by authorized users, regardless of their physical location.
CCE1.12.1: The AECCE should support access to mission / business applications and data via an attribute-based access control (ABAC) methodology. Data owners should clearly state their access control rules in terms of user attributes.
CCE1.13: Mission / Business applications are executable within the Computing Environments (CE) defined in the COE.
CCE1.13.1: AECCE will closely adhere to approved and emerging DoD IT Standards Registry (DISR) standards and/or the standards listed in the COE StdV-1 and StdV-2 to enable enterprise & Army specific services and approved end-user devices. Compliance and conformance to the DISR and Reference Architecture will be managed by CIO/G6 and where necessary/justified wavers will be issued.
CCE1.14: Application services must be monitored to ensure users are able to accomplish their missions effectively and efficiently
CCE1.14.1: ARCYBER/2nd Army will establish a Service Desk to monitor performance of platform services provided by CSPs and to identify, report, track and resolve information technology faults, incidents, and problems within the AECCE per signed SLA/MOA/MOU.
CCE1.14.2: Application/System owners are responsible for deploying, configuring, updating, and managing the operations of an application including data when using PaaS.
CCE1.14.3: Application owner is responsible for application performance, tuning, patch management, and configuration management when using PaaS. Application performance is a shared responsibility between the application owner and the Cloud Service Provider IAW the SLA/MOA/MOU.

Table 6 - Services Management

3.2.1 Assumptions

None identified at this time.

3.2.2 Risks

- Loss of application/system functionality during the execution of the application migration.
- Data migration and management may cause data loss
- Overcoming network challenges between enterprise and edge users
- Unforeseen or unplanned power outages and system downtime
- Data corruption and data loss
- Data security, data quality and data integrity
- Current organizational structures and funding processes may not be optimal for enterprise cloud service procurement, implementation, and management
- Current Army operational requirements may preclude taking full advantage of cloud capabilities
- Continuity of CSP during migration/transition of applications and data.
- Army organization may fail in its mission because of non-compliance with CSP's SLA or because of application/service performance failure.

3.3 Operate and Defend the AECCE

Cybersecurity is an increased concern to the DOD and the Army in a virtualized environment. The focus of this capability is strengthening Network and Cybersecurity by supporting continuous monitoring; and integrating identity and access management.

CCE1.15: AECCE products and services allow a high degree of automation for NetOps C2 and support dynamic adjustment of configuration and resource allocation. (DOD IEA, V2.0, Vol. II, B-6, NOAR 05)
CCE1.15.1: AECCE infrastructure, applications and services, network resources, enclaves, and boundaries shall be capable of being configured and operated in accordance with applicable DoD and Army policy. Such policy must address differences in enterprise-wide, system high, community of interest, enclave, and operational mission needs. (DOD IEA, V2.0, Vol. II, B-3, SAR 02)
CCE1.15.2: The AECCE instantiations should ensure that configuration changes to networks, data assets, services, applications, and device settings can be automatically disseminated and implemented in conformance with GIG-standard configuration processes. (DOD IEA, V2.0, Vol. II, B-4, SAR 10)
CCE1.15.3: AECCE NetOps capabilities will enable dynamic optimization of the flow of data/information.
CCE1.15.4: AECCE NetOps capabilities will enable management and control of operational IT components to optimize the efficiency and effectiveness of IT service delivery to end-users.
CCE1.15.5: AECCE NetOps will be capable of resolving resource contention in the use of network capacity in accordance with Army policy, service-level agreements, quality-of-service guidelines, etc.
CCE1.15.6: NetOps functionality within AECCE will be managed by a single organization entity that has access to all AECCE operational and status data.

Table 7 - Operate the AECCE

CCE1.16: All AECCE services that enable the sharing or transfer of information across multiple security levels shall be centrally planned and coordinated, with proposed service enhancements considered first at the enterprise-wide level, then at the regional/organizational level, then at the service or application level. (DOD IEA, V2.0, Vol. II, B-3, SAR 06)
CCE1.16.1: AECCE will enable collaborative information sharing across network boundaries in accordance with DOD standards, guidelines, policies and Army Regulation (AR) 25-2.
CCE1.16.2: AECCE infrastructure (computing and network), programs, and applications shall protect data in transit and at rest according to their confidentiality level, Mission Assurance category, and level of exposure. (DOD IEA, V2.0, Vol. II, B-3, SAR 01)
CCE1.16.3: AECCE will, where required, implement appropriate cross-domain solutions to support encrypted data transport between internal and external networks for information sharing.
CCE1.17: An AECCE characteristic is strong authentication for person and non-person entities to allow only authorized users access to information and data by validating their credentials/attributes.
CCE1.17.1: All entities authorized to access AECCE instantiations will have one identity and universal credentials that are recognized by all producers of information and services. (DOD IEA, V2.0, Vol. II, B-7, OPR 01)
CCE1.17.2: AECCE will support roaming profiles optimized to the warfighter environment allowing them access to their information and services (e.g. data files, personal files, calendar, contact list, email, etc). (DOD IEA, V2.0, Vol. II, B-7, OPR 13)
CCE1.17.3: AECCE will leverage the Enterprise IdAM implementation for enablement of strong authentication of person and non-person entities to validate authorization for access to information and data.
CCE1.17.4: Cloud consumer and machine authentication will leverage the current DOD PKI solution and all digital certificates will comply with the current ITU-T X.509 standard.
CCE1.18: AECCE provides sufficient operational and status data so that complete cybersecurity situational awareness can be achieved.
CCE1.18.1: AECCE instantiations will support NetOps tools and processes in identifying, isolating, and resolving problems that either reduce network availability or impair the ability of end-users to use AECCE.
CCE1.18.2: AECCE will implement an attribute-based access control (ABAC) methodology to control access to its resources.

Table 8 - Defend the AECCE

3.3.1 Assumptions

- Federal Risk and Authorization Management Program (FedRAMP), Risk Management Framework and DOD-identified security controls provide the foundation for a standard approach to assessing and authorizing cloud computing services.
- Cloud implementation will align with updated DOD cybersecurity policies and instructions, and cybersecurity controls and processes.
- The security controls required in a cloud environment will be enforced IAW FedRAMP and NIST and DOD security guidelines.
- Requirements for continuous auditing/monitoring of cloud service providers are necessary.
- Detecting failures, understanding their consequences, isolating their effects, and remediating risks are central to the adoption of cloud computing environment.
- New applications are designed to be resilient and to withstand failure of one or more elements of the cloud infrastructure

3.3.2 Risks

None identified at this time.

3.4 Govern and Manage AECCE

This activity identifies and enforces the required vision, strategy, and guidance to direct the AECCE so it meets requirements and applicable law, regulation, and policy (LRP), while at the same time delivering the capabilities necessary to fully enable net-centric warfighting, business, and defense intelligence operations for successful mission accomplishment. It establishes and uses structures and processes required to provide effective, high-level management and oversight of the components of the AECCE and its operations.

CCE1.19: The Army achieves infrastructure interoperability through definition and enforcement of standards, interface profiles and implementation guidance. (DOD IEA, V2.0, Vol. II, B-1, GP 02)
CCE1.19.1: The AECCE is a capability managed within the Army Enterprise Network Portfolio (AENP) and requirements validation and policy guidance for the AECCE will be the responsibility of the Army Enterprise Network Council.
CCE1.19.2: Data Centers under Army Executive Agency will comply with DOD/JIE mandated Standards and guidelines, and be able to federate with other DOD and non-DOD facilities hosting the AECCE.
CCE1.19.3: AECCE will integrate with DOD, DISA, and JIE Cloud Computing capabilities and adhere to associated guidelines, directives, and standards to achieve data and information sharing, interoperability and portability.
CCE1.19.4: Existing Army applications and its data will be modified, when necessary, to be cloud enabled to operate in a cloud computing environment and migrated to an appropriate data center to improve efficiencies,
CCE1.19.5: New Army applications will be designed and developed to be cloud optimized and take full advantage of functioning in a cloud computing environment to include the ability to withstand infrastructure component failure without degrading application availability or performance and making use of PaaS capabilities as appropriate
CCE1.19.6: Legacy applications may exist in a non-virtualized / non-cloud environment with an approved waiver. The approval authority for all waivers is the Army CIO/G-6

Table 9 - Standards and Policy

CCE1.20: Army will consolidate computing infrastructure by consolidating data centers and virtualizing servers and applications as a precondition for cloud migration.
CCE1.20.1: AECCE will provide a highly automated computing infrastructure, limiting the need for human intervention and enabling the optimization of computing infrastructure resources.
CCE1.20.2: ASA (ALT) will, in coordination with the CIO/G-6, develop an overarching infrastructure acquisition strategy (hardware, software, etc) and enforce common computing infrastructure standards.
CCE1.20.3: Army Cyber Command (ARCYBER) and 2nd Army will establish and maintain Regional Combatant Command (CCMD)-aligned network service centers to shift from a Service-centric network construct to an operational (i.e., regional) construct supporting regional unified operations within the JIE
CCE1.20.4: Application developers will adopt virtualization technology to reduce excess hardware and for consolidating infrastructure.
CCE1.20.5: Application Manager/owner will develop a detailed plan for modernization of applications identified for transition to a cloud computing environment to identify the issues that can be resolved before the migration.
CCE1.20.6: As a pre-condition, application owner will identify, record, and describe rationalization results and status of their application's functionality, characteristics, and current status in the ADCCP Tracking Tool.

Table 10 - Processes and Models

CCE1.21: Cloud Service Providers and consumers will establish SLAs for all services provided within the AECCE.
CCE1.21.1: As a minimum SLAs should include but are not limited to the following topics: ○ Availability ○ Backup Power Sources ○ Remedies for Failure to Perform ○ Data Preservation/Retention ○ Legal Care of Consumer Information ○ Scheduled Outage ○ Force Majeure Events ○ Service Agreement Change ○ Security, Criticality, and Backup ○ Service API Change ○ Acceptable Use Policies ○ Licensed Software ○ Timely Payments ○ Termination Policy ○ Access to usage and performance metrics ○ Application Failover Policy ○ Application Virtual Resource Requirements ○ Application Performance Requirements

Table 11 - Monitoring and Compliance

3.4.1 Assumptions

None identified at this time.

3.4.2 Risks

None identified at this time.

4. Summary

The objectives of Version 1 of this RA are to standardize Army Cloud Computing implementations and provide guidance in transitioning to cloud computing environments. The achievement of these objectives has the expected benefits of reduction in IT costs, better response to user needs, and improved security. Version 2 of this RA will be released in FY15. Version 2 will focus on data storage management within the AECCE and detailed modernization of applications and data migration processes. As it is additive, principles and rules provided in this version will be updated to reflect new guidance from leadership, lessons learned from pilot activities, and revisions to current Federal, DOD and Army strategies, architectures and policies.

Appendix A - StdV-1 Standards View

A StdV-1 is "The listing of standards that apply to solution elements."
Note: The table below is not an exhaustive list of DOD IT Standards Registry (DISR) and industry standards pertain to cloud computing. As the cloud standards mature overtime, the CIO/G6 (in coordination with DOD and acquisition community) will submit DISR Change Requests for the applicable non-DISR/non-Mandated standards. In addition to CIO/G6's guidance, solution providers will ensure compliance with the current DOD/Joint policies when developing Information Support Plans & StdV-1/2.

Name	Version	Sponsoring Body	Recommended DISR Status	Description
Cloud Data Management Interface (CDMI)	1.0.2	ISO/IEC and SNIA	Mandated	Defines the functional interface that applications will use to create, retrieve, update, and delete data elements from the Cloud.
Open Virtualization Format (OVF)	1.1.0	ANSI, ISO, DMTF	Mandated	Describes an open format for the packaging and redeployment of virtual machines. The specification also defines Conformance levels, which describe the inclusion of custom elements that may impact portability.
Open Virtualization Format (OVF)	2.0	DMTF	Emerging	The second version of the standard, OVF 2.0, which applies to emerging cloud use cases and provides important developments from OVF 1.0, including improved network configuration support and package encryption capabilities for safe delivery.
Virtual Machine Disk (VMDK)	1.1	VMWare	Mandated	The format is a container for virtual hard disk drives to be used in virtual machines.
Cloud Infrastructure Management Interface(CIMI)	1.0.0	DMTF	Emerging	Provides a self-service interface for infrastructure clouds, allowing users to dynamically provision, configure, and administer their cloud usage using a high-level interface that abstracts away much of the complexity of systems management.
Common Information Model Infrastructure (CIM-Infrastructure)	2.7.0	DMTF	Emerging	Applies the basic structuring and conceptualization techniques of the object-oriented paradigm.
Data Format Description Language (DFDL)	1.0	Open Grid Forum (OGF)	Emerging	Used to describe formatting of text or binary data.
Open Cloud Computing Interface –	1.1	OGF	Emerging	Three distinct standards (Core, Infrastructure, HTTP) that allow the creation of tools for interoperability and

Name	Version	Sponsoring Body	Recommended DISR Status	Description
Infrastructure (OCCI)				portability functions like semantic renderings, monitoring, billing, reservations and service negotiation/agreement.
Open Data Protocol (oData)	1.0	OASIS	Emerging	Simplifies the querying and sharing of data across disparate applications and multiple stakeholders for re-use in the enterprise, cloud, and mobile devices. REST-based; builds on HTTP.
Topology and Orchestration Specification for Cloud Applications (TOSCA)	1.0	OASIS	Emerging	Enhances the portability of cloud applications and services. Enables the interoperable description of application and infrastructure cloud services, the relationships between parts of the service, and the operational behavior of these services – independent of the supplier creating the service and any particular cloud provider or hosting technology.

Appendix B - AV-2 Vocabulary (Integrated Dictionary)

An Av-2 is “An architectural data repository with definitions of all terms used throughout the architectural data and presentations.”

Term	Definition
Application Management	It is the process of managing the operation, maintenance, versioning and upgrading of an application throughout its lifecycle.
Availability Management	Manage the availability of IT services through definition, analysis, planning, measurement, and improvement as the party responsible for ensuring that all IT infrastructure, processes, tools, and roles are appropriate for established service-level targets.
Backup and Recovery	Backup and recovery refers to the process of backing up data in case of a loss and setting up systems that allow data recovery due to a data loss. Backing up data requires copying and archiving computer data, so that it is accessible in case of data deletion or corruption. Data from an earlier time may only be recovered if it has been backed up. Data backup is a key element of disaster recovery and should be part of any disaster recovery plan.
Backward Compatible	The ability of a software program or piece of hardware to read files in previous versions of the software or hardware. (DOD 5015.02-STD) April 25, 2007
Broad Network Access	Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
Business Rules	Business rules are definitive statements that provide design tenets and also constrain the implementation of principles and associated policies, as well as acquisition guidance. Business rules represent relationships among the AECCE inputs, controls, outputs, and the mechanisms and resources used. For example, a business rule can specify who can do what under specified conditions, the combination of inputs and controls needed, and the resulting outputs. AECCE business rules are based on best practices, provide design tenets, and constrain the implementation of principles and relevant policies.
Capacity Management	Provide a process for ensuring that IT services and IT infrastructure are able to deliver established service-level targets in a cost-effective and timely manner.
Change Management	Provide control of the lifecycle of all changes to enable beneficial modifications to be made with minimum disruption of enterprise-level IT services.
Client	A hardware device or software application that requests and makes use of services provided by another computer called the server.
Cloud Broker	An individual or organization that consults, mediates and facilitates the selection of cloud computing solutions on behalf of an organization. A cloud broker serves as a third party between a cloud service provider and organization buying the provider's products and solutions.
Cloud Computing (NIST)	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. (Source: NIST Special Publication 800-145)
Cloud consumer / customer / subscriber / user	A person or organization that maintains a business relationship with, and uses services from, Cloud Providers.
Cloud Interoperability	Refers to the ability to manage cloud based applications that exist across

Term	Definition
	two or more cloud hosting environments, preferably using a unified management tool set. This is particularly useful when implementing hybrid cloud solutions.
Cloud Management	Cloud management is the process of evaluating, monitoring and optimizing cloud computing based solutions and services to produce the desired efficiency, performance and overall service level required. Cloud management is the practice of end-to-end supervision of the cloud environment by an organization, cloud service vendor or both. It ensures that the cloud computing services are delivered and operated in the most optimal form.
Cloud Portability	The ability to move applications packaged as Virtual Machines (VMs) from one cloud computing environment to another with little or no modification to the application or VM.
Cloud Provider / Cloud Service Provider (CSP)	An organization (e.g., a company or other possibly government organization) that delivers cloud computing based services and solutions to businesses, organizations, and/or individuals. This service organization may provide rented and provider-managed virtual hardware, software, infrastructure and other related services.
Collaboration	The ability to conduct synchronous and asynchronous communications and interaction across the enterprise, including voice, data, video, and manipulated visual representation.
Common Operating Environment	An approved set of IT components (hardware and/or software) and IT technologies whose use is intended to facilitate the Army's ability to rapidly develop, integrate, certify, and deploy secure and interoperable IT systems and applications.
Community Cloud	The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
Computing Environment	A logical grouping of systems with similar deployment and environmental characteristics used to organize the Common Operating Environment. The six Computing Environments are: Data Center / Cloud, Command Post, Mounted, Mobile / Handheld, Sensor, and Real-Time / Safety Critical / Embedded.
Configuration Management	Refers to a discipline for evaluating, coordinating, approving or disapproving, and implementing changes in artifacts that are used to construct and maintain software systems. An artifact may be a piece of hardware or software or documentation. CM enables the management of artifacts from the initial concept through design, implementation, testing, baselining, building, release, and maintenance.
Content Management (CM)	The administration of digital content throughout its lifecycle, from creation to permanent storage or deletion. The content involved may be images, video, audio and multimedia as well as text.
Continuity of Operations Program (COOP)	A set of policies, plans, procedures, and capabilities that provides for the continued execution of critical missions and functions across a wide range of potential emergencies, including localized acts of nature, accidents, technological, and or attack related emergencies. [Definition per Army Regulation (AR) 500-3, U.S. Army Continuity of Operations Program Policy and Planning, Section II, Terms, 18 April 2008.] LWN Services Catalog v2 Oct 2013
Core Data Center (CDC)	A CDC is a fixed DOD data center meeting DOD standards for facility and network infrastructure, security, technology, and operations and adhering to enterprise governance. Functions and services delivered by current

Term	Definition
	DISA DECCs, Component Enterprise DCs and Component Installation DCs will be consolidated to the greatest extent possible into Core DCs totaling a few dozen at most. CDCs will be selected from existing Component data centers. (Draft DC RA)
Directory Services	Software systems that store, organize and provide access to directory information in order to unify network resources. Directory services map the network names of network resources to network addresses and define a naming structure for networks.
Enterprise Cross Domain Services	Enterprise Cross Domain Services (ECDS) - An automated set of capabilities available to multiple end users, organizations, and/or hosted mission applications within an enterprise environment for information sharing across and among security domains utilizing one or more cross domain solutions(CNSSI 4009)
Enterprise Service	A set of one or more computer applications and middleware systems hosted on computer hardware that provides standard information systems capabilities to end users and hosted mission applications and services. (CNSSI 4009, pg 28)
Enterprise Services	The ability to provide to all authorized users awareness of and Access to all DOD information and DOD-wide information services. (DOD Enterprise Services Management Frame work, (DESMF))
Federated Cloud	The deployment and management of multiple external and internal cloud computing services to match business needs.
Force majeure events	An event or effect that cannot be reasonably anticipated or controlled.
Guiding Principles	Guiding Principles are high-level statements that apply to the subject area and tie back to requirements. Reference architecture principles are enduring guidelines that describe how capabilities will fulfill a mission. Principles express the intent of the capability and fundamental values to be achieved.
Hybrid Cloud	The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).
Hypervisor	A hypervisor, also called a virtual machine manager, is a program that allows multiple operating systems to share a single hardware host. Each operating system appears to have the host's processor, memory, and other resources all to itself. However, the hypervisor is actually controlling the host processor and a resource, allocating what is needed to each operating system in turn, and making sure that the guest operating systems (called virtual machines) cannot disrupt one another.
Incident Management	Provide a management process to restore normal service operation (as defined with SLAs) as quickly as possible, while minimizing adverse effect on operations, ensuring that the best possible levels of service quality and availability are maintained.
Infrastructure as a Service (IaaS)	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).
Installation Processing Node (IPN)	An IPN is a fixed (i.e., not designed to be relocated or transported) data center serving a single installation or several installations in a defined area (e.g., a Joint Base). An IPN hosts applications and services that

Term	Definition
	cannot otherwise be relocated to or serviced by a CDC;
IT service	A service provided to one or more customers by an IT Service Provider. An IT service is based on the use of Information Technology and supports the Customer's Business Processes. An IT Service is made up from a combination of people, processes and technology and should be defined in a Service Level Agreement.
Measured Service	Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.
Middleware	Software that acts as a bridge between an operating system or database and applications, especially on a network. High-level host server operating system software used to control virtual operating systems
On-demand Self-service	A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
Patterns	Patterns are generalized architecture representations/viewpoints, graphical/textual models, diagrams, etc., that show relationships among elements and artifacts specified by the technical positions.
Platform as a Service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
Portability	The ability to transfer data from one system to another without being required to recreate or reenter data descriptions or to modify significantly the application being transported.
Private Cloud	The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
Public Cloud	The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
Rapid Elasticity	Capabilities can be rapidly and elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
Reference Architecture (RA)	Reference Architecture is an authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions – Office of the Secretary of Defense, Networks and Information Integration, Reference Architecture Description, June 2010.
Resource pooling	The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Term	Definition
Risk	Risks are technical, political, cultural and governance inhibitors that conflict with guiding principles and target business rules. They are factors that would significantly impact the realization of a Business Rule. Risks include risk to the mission, operations, compliance, strategic direction, investments, service delivery, information assurance, manpower, and others. In other words, risks include anything that could impact the strategic objectives and operational readiness of the organization the governance body directs and controls. (DESF, Edition II)
Service	Service is comprised of a range of products, processes and people perceived by mission partners and users as a self-contained, single, coherent entity that enables them to achieve mission objectives and functions. (DESF) Edition II.
Service Desk	The Single Point of Contact between the Service Provider and the Users. A typical Service Desk manages Incidents and Service Requests, and also handles communication with the Users.
Service Level Agreement (SLA)	A legal document specifying the rules of the legal contract between a subscriber and provider stating technical performance promises made by a provider including remedies for performance failures.
Service Management	Provide process-focused management for Army/DOD enterprise IT systems focused on providing a framework to structure IT-related activities and the interactions of IT technical personnel with Enterprise users.
Service Owner	Organization responsible for overall management and governance of the service
Service Provider	Organization responsible for hosting and delivery of the service to authorized consumers
Service Support	Provide support services for ensuring that users have Access to the appropriate services to support mission functions.
Software as a Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
Technical Positions	Technical Positions are a minimal set of enduring technical standards arranged and associated to guide implementation; a set of core or critical technical standards required to establish the capabilities required a Business Rule. Technical positions describe the technical guidance and standards established for Army cloud computing environment. This technical guidance documentation allows for system owners' and PEOs/PMs' justification to resource their systems, and identifies potential choices and tradeoffs to perform.
Testing	Activity that verifies that a Configuration Item, IT Service, Process, etc. meets its Specification or agreed Requirements.

Appendix C - Acronyms

Acronym	Definition
ABAC	Attribute Based Access Control
ADCCP	Army Data Center Consolidation Program
AECCE	Army Enterprise Cloud Computing Environment
AECCRA	Army Enterprise Cloud Computing Reference Architecture
AEN	Army Enterprise Network
AENP	Army Enterprise Network Portfolio
AIA	Army Information Architecture
AIC	Army Interoperability Certification
AIS	Automated Information Systems
AMC	Army Materiel Command
AR	Army Regulation
ARCYBER	Army Cyber Command
ASA(ALT)	Assistant Secretary of the Army (Acquisition, Logistics and Technology)
ASCC	Army Service Component Commands
AV	All View
BMA	Business Mission Area
BR	Business Rule
C2	Command and Control
CCE	Cloud Computing Environment
CDC	Core Data Center
CE	Computing Environment
CI	Computing Infrastructure
CIO	Chief Information Officer
CIRP	Computing Infrastructure Readiness Principles
CIRR	Computing Infrastructure Readiness Rules
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CM	Content Management
CM	Configuration Management
CND	Computer Network Defense
CNSSI	Committee on National Security Systems Instruction
COE	Common Operating Environment
COI	Community of Interest
CONOPS	Concept of Operations
CONUS	Continental United States
COOP	Continuity of Operations Program
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
CR	Change Request
CRP	Communications Readiness Principle
CRR	Communications Readiness Rule
CSP	Cloud Service Provider
CV	Capability View
DAPam	Department of the Army Pamphlet

Acronym	Definition
DC	Data Center
DECC	Defense Enterprise Computing Center
DIACAP	DOD Information Assurance Certification and Accreditation Process
DIEA	DOD Information Enterprise Architecture
DIL	Disconnected, Intermittent, Low-bandwidth
DISA	Defense Information Systems Agency
DISR	DOD IT Standards Registry
DOD	Department of Defense
DOD IEA	DOD Information Enterprise Architecture
DOD ITER	DOD IT Enterprise Roadmap
DODAF	DOD Architecture Framework
DODI	DOD Instruction
DODIN	DOD Information Network
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities.
DSDP	Data & Services Deployment Principle
DSDR	Data & Services Deployment Business Rules
EA	Enterprise Architecture
EAs	Enterprise Applications
EM	Enterprise Management
EoIP	Everything Over Internet Protocol
ERP	Enterprise Resource Program
ESD	Enterprise Services Domain
FedRAMP	Federal Risk and Authorization Management Program
FIPS PUB	Federal Information Processing Standards Publication
FORSCOM	Forces Command
GAO	Government Accountability Office
GIG	Global Information Grid
H/W	Hardware
HQDA	Headquarters Department of the Army
HTTP	Hyper Text Transfer Protocol
IA	Information Assurance
IAA	Inter-Agency Agreement
IaaS	Infrastructure as a Service
IAW	In accordance with
IC ITE	Intelligence Community Information Technology Enterprise
IdAM	Identity and Access Management
IE	Information Enterprise
IEA	Information Enterprise Architecture
IM	Information Management
INSCOM	Intelligence and Security Command
IPN	Installation Processing Node
IPv	Internet Protocol Version
ISN	Installation Service Node
IT	Information Technology
ITESR	IT Enterprise Strategy and Roadmap
ITSM	Information Technology Services Management

Acronym	Definition
ITU	International Telecommunications Union
JCA	Joint Capability Area
JCIDS	Joint Capabilities Integration and Development System
JIE	Joint Information Environment
LWN	LandWarNet
MA	Mission Assurance
MAs	Mission Areas
MEF	Mission Essential Functions
MOA	Memorandum of Agreement
MOE	Measures of Enhancements/Effectiveness
MOPS	Measures of Performance
MOU	Memorandum of Understanding
MPLS	Multiprotocol Label Switching
NCD	Network Capacity Domain
NCS	Network Capability Sets
NDAA	National Defense Authorization Act
NETCOM	Network Enterprise Technology Command/9th Signal Command
NetOps	Network Operations
NGO	non-governmental organization
NIPRNet	Non-Secure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NMA	Network Mission Area
NOAP	NetOps Agility Principles
NOAR	NetOps Agility Rules
NSA	National Security Agency
NSD	Network Operations and Security Domain
NSS	National Security Systems
OM	Operations and Maintenance
OMB	Office of Management and Budget
OPR	Derived Operational Rules
OS	Operating System
OV	Operational View
PaaS	Platform as a Service
PEO	Program Executive Officers
PKI	Public Key Infrastructure
PM	Program Manager
PR	Principle
RA	Reference Architecture
RAMP	Risk Assessment and Management Plan
RBA	Rules-Based Architecture
REST	Representational State Transfer
RM	Reference Model
RMF	Risk Management Framework
RSS	Regional Security Stacks
SaaS	Software as a Service

Acronym	Definition
SAP	Secured Availability Principles
SAR	Secured Availability Rules
SECArmy	Secretary of the Army
SIP	Shared Infrastructure Principles
SIPRNet	Secret Internet Protocol Router Network
SIR	Shared Infrastructure Business Rules
SLA	Service Level Agreement
SOP	Standard Operating Procedures
SPPN	Special Purpose Processing Node
SSA	Single Security Architecture
STD	Standard
StdV	Standards View
SV	Systems View
SW	Software
TPN	Tactical/Mobile Processing Node
TRADOC	Training and Doctrine Command
TTPs	Tactics Techniques and Procedures
UC	Unified Capabilities
UCP	Unified Command Plan
VDI	Virtual Desktop Infrastructure

Appendix D - References

The references listed below are general references that are applicable to the Army Enterprise operations and the AECCRA:

1. Office of the Assistant Secretary of Defense, Networks and Information Integration (OASD/NII) Reference Architecture Description, June 2010 http://dodcio.defense.gov/Portals/0/Documents/DIEA/Ref_Archi_Description_Final_v1_18Jun10.pdf
2. DoD Information Enterprise Architecture (IEA) v2.0, Jul 2012 http://dodcio.defense.gov/Home/Initiatives/DIEA.aspx
3. Army CIO/G-6, LandWarNet 2020 and Beyond Enterprise Architecture, v2.0, 1 August 2014 http://ciog6.army.mil/Architecture/tabid/146/Default.aspx/
4. Army CIO/G-6, Annex A, Technical Standards Guidance to LandWarNet 2020 and Beyond Enterprise Architecture, v2.0, 1 August 2014
5. Army CIO/G-6, Definitions and Guidance for the Common Operating Environment, Annex B to LandWarNet 2020 and Beyond Enterprise Architecture, v2.0, 1 August 2014
6. IC IT Enterprise Fact Sheet, Defense National Intelligence, CIO http://www.dni.gov/files/documents/IC%20ITE%20Fact%20Sheet.pdf
7. DOD Cloud Computing Strategy, 9 January 2012 http://www.defense.gov/news/dodcloudcomputingstrategy.pdf
8. National Institute of Standards and Technology (NIST), Special Publication 800-145, The NIST Definition of Cloud Computing, September 2011 http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
9. Director, Architecture & Interoperability, Office of the DoD Chief Information Officer, Core Data Center Reference Architecture, Version 1.0, September 18,2012 http://dodcio.defense.gov/Portals/0/Documents/DIEA/CDC%20RA%20v1_0_Final_Releaseable%20Version.pdf
10. Federal Risk and Authorization Management Program (FedRAMP) http://cloud.cio.gov/sites/default/files/documents/files/FedRAMP%20Security%20Assessment%20Framework%20v1.0.docx http://cloud.cio.gov/fedramp/cloud-systems
11. DOD Enterprise Cloud Service Broker, http://www.disa.mil/Services/DoD-Cloud-Broker
12. DOD “Joint Information Environment: Continental United States Core Data Centers and Application and System Migration” 11 Jul 2013
13. ASA(ALT) COE Data Center/Cloud Computing Environment Architecture Addendum; v2.0.2, 1 June 2014 https://www.intelink.gov/go/BIS90fr
14. ASA(ALT) COE Data Center/Cloud Computing Environment Architecture Compliance document, v2.0.2, 1 June 2014 https://www.intelink.gov/go/71pxBsF
15. Federal Data Center Consolidation Initiative, Department of Defense 2011 Data Center Consolidation Plan & Progress Report, November 8, 2011 http://dodcio.defense.gov/Portals/0/Documents/FDCCI-Final-2011.pdf
16. Under Secretary of the Army Memorandum, Subject: Migration of Army Enterprise Systems/Applications to Core Data Centers, dated 9 Jun 2014.

https://west.esps.disa.mil/army/cmds/hqda_ciog6_Project/ADCCP/SitePages/Home.aspx?InitialTabId=Ribbon%2EDocument&VisibilityContext=WSSTabPersistence

17. DOD Cloud Way Forward, Version 1.0, 23 July 2014 https://software.forge.mil/sf/docman/do/listDocuments/projects.dodcloud/docman.root.dod_cloud_mildep_js_disa_cio_wg.13_august_2014
18. Federal Cloud Computing Strategy, 8 February 2011 https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf
19. Army Regulation 25-2, Information Assurance, Rapid Action Revision (RAR), 23 March 2009, http://www.apd.army.mil/pdffiles/r25_2.pdf
20. NIST, Special Publication 500-291,Cloud Computing Standards Roadmap, July 2011 http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909024
21. NIST, Special Publication 500-292, Cloud Computing Reference Architecture, September 2011 http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505
22. NIST, Special Publication 800-146, Cloud Computing Synopsis and Recommendations, May 2012 http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf
23. AR 500-3, U.S. Army Continuity of Operations Program Policy and Planning, 18 April 2008 http://www.apd.army.mil/pdffiles/r500_3.pdf
24. Army CIO/G-6, Army Cloud Computing Strategy, to be published 1st Quarter FY 15