The Army Cloud Computing Strategy

What is it?

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 information technology (IT) infrastructure, systems, software and application platforms; data assets; and related business processes and practices. It is the overarching plan for the transition to cloud-based solutions.

The Army Cloud Computing Strategy is designed to establish and communicate the Army's vision and strategy for transitioning to a cloud-enabled network, to improve mission and business effectiveness, increase operational IT efficiencies and protect Army data and infrastructure. The strategy extends the baseline and concepts defined in the various federal, DoD and Army documents to meet specific Army requirements.

What has the Army done?

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

Why is this important to the Army?

Cloud technology has great utility for the military. Cloud computing will increase the capabilities and responsiveness of both the generating and operating forces 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 Joint Information Environment. 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 point of need.

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 IT. Procuring these as services will allow the Army to focus resources more effectively to meet evolving mission needs. Over time it 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.

What continued efforts does the Army have planned for the future?

The Army will implement modernization plans and develop processes and procedures to leverage approved DoD, federal and commercial cloud service providers, and ensures offerings align to mission requirements and provide the minimum set of security controls necessary to protect critical information against known and

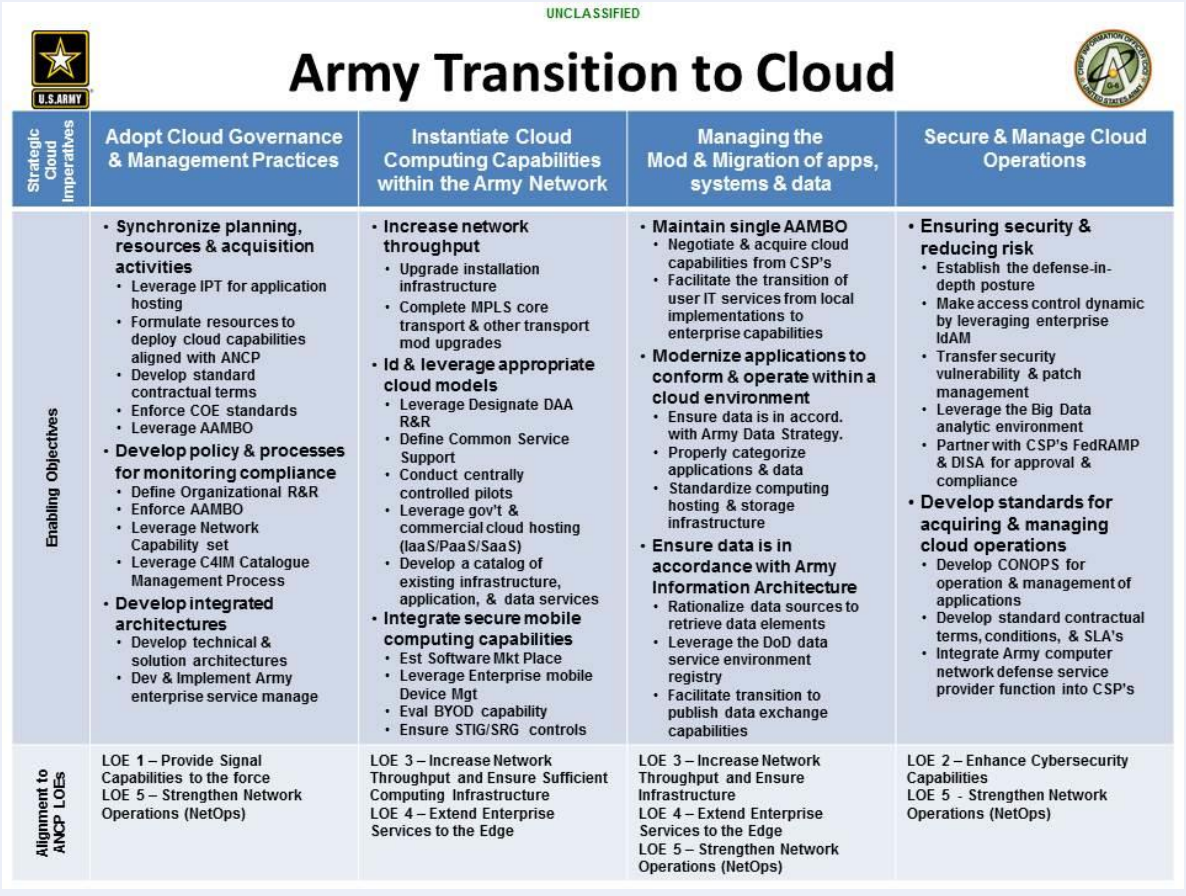
References to any commercial products, processes, or services, or the use of any trade, firm or corporation name is for the information and convenience of the public, and does not constitute an endorsement, recommendation, or preferential treatment by the U.S. Army.

emerging threats. The transition to cloud-based solutions and services will enable the Army to successfully provide the robust network necessary for our warfighters anytime, anywhere.

The Army CIO/G-6 is currently working on a Commercial Cloud Services Provider policy guidance to be published within the coming weeks. This policy guidance supports the Under Secretary of the Army memorandum that was published 09 June 2014 and DoD CIO memorandum that was published 15 December 2014. It reinforces rationalization, identifies systems and applications not permitted to migrate to off-premises commercial CSPs, outlines requirements for acquisition and use of commercial CSPs, and provides a high-level overview of the Army applications migration process flow.

How will the Army turn to cloud computing and ensure all data to include unclassified and classified information is secured on the cloud?

It is important to note that the Army Cloud Computing Strategy does not cross into the Intelligence community or the Joint Worldwide Intelligence Community System. Army Intelligence will continue to maintain data classified above the Secret level and must comply with Intelligence Community requirements to secure that data. Army Intelligence data resources will also continue to comply with Intelligence Community data governance standards and requirements.


UNCLASSIFIED

Army Transition to Cloud

Strategic Cloud Imperatives	Adopt Cloud Governance & Management Practices	Instantiate Cloud Computing Capabilities within the Army Network	Managing the Mod & Migration of apps, systems & data	Secure & Manage Cloud Operations

Enabling Objectives	• **Synchronize planning, resources & acquisition activities**
	  • Leverage IPT for application hosting
	  • Formulate resources to deploy cloud capabilities aligned with ANCP
	  • Develop standard contractual terms
	  • Enforce COE standards
	  • Leverage AAMBO
	• **Develop policy & processes for monitoring compliance**
	  • Define Organizational R&R
	  • Enforce AAMBO
	  • Leverage Network Capability set
	  • Leverage C4IM Catalogue Management Process
	• **Develop integrated architectures**
	  • Develop technical & solution architectures
	  • Dev & Implement Army enterprise service manage
		• **Increase network throughput**
		  • Upgrade installation infrastructure
		  • Complete MPLS core transport & other transport mod upgrades
		• **Id & leverage appropriate cloud models**
		  • Leverage Designate DAA R&R
		  • Define Common Service Support
		  • Conduct centrally controlled pilots
		  • Leverage gov't & commercial cloud hosting (IaaS/PaaS/SaaS)
		  • Develop a catalog of existing infrastructure, application, & data services
		• **Integrate secure mobile computing capabilities**
		  • Est Software Mkt Place
		  • Leverage Enterprise mobile Device Mgt
		  • Eval BYOD capability
		  • Ensure STIG/SRG controls
			• **Maintain single AAMBO**
			  • Negotiate & acquire cloud capabilities from CSP's
			  • Facilitate the transition of user IT services from local implementations to enterprise capabilities
			• **Modernize applications to conform & operate within a cloud environment**
			  • Ensure data is in accord. with Army Data Strategy.
			  • Properly categorize applications & data
			  • Standardize computing hosting & storage infrastructure
			• **Ensure data is in accordance with Army Information Architecture**
			  • Rationalize data sources to retrieve data elements
			  • Leverage the DoD data service environment registry
			  • Facilitate transition to publish data exchange capabilities
				• **Ensuring security & reducing risk**
				  • Establish the defense-in-depth posture
				  • Make access control dynamic by leveraging enterprise IdAM
				  • Transfer security vulnerability & patch management
				  • Leverage the Big Data analytic environment
				  • Partner with CSP's FedRAMP & DISA for approval & compliance
				• **Develop standards for acquiring & managing cloud operations**
				  • Develop CONOPS for operation & management of applications
				  • Develop standard contractual terms, conditions, & SLA's
				  • Integrate Army computer network defense service provider function into CSP's

Alignment to ANCP LOEs	LOE 1 – Provide Signal Capabilities to the force LOE 5 – Strengthen Network Operations (NetOps)	LOE 3 – Increase Network Throughput and Ensure Sufficient Computing Infrastructure LOE 4 – Extend Enterprise Services to the Edge	LOE 3 – Increase Network Throughput and Ensure Infrastructure LOE 4 – Extend Enterprise Services to the Edge LOE 5 – Strengthen Network Operations (NetOps)	LOE 2 – Enhance Cybersecurity Capabilities LOE 5 - Strengthen Network Operations (NetOps)

Resources:
Army Network Campaign Plan
Army Cloud Computing Strategy
UnderSec Army Memo, Migration of Army Enterprise Sys/Apps to Core Data Centers

References to any commercial products, processes, or services, or the use of any trade, firm or corporation name is for the information and convenience of the public, and does not constitute an endorsement, recommendation, or preferential treatment by the U.S. Army.