



DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

Office, Chief Information Officer/G-6

JUL 23 2015

SAIS-AOC

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Guidance for Migration to, and Use of, Commercial Cloud Service Providers (CSPs)

1. References: See Enclosure 1.
2. Purpose. To provide guidance for migration to, and use of, CSPs. This guidance supports policy and requirements issued by the Under Secretary of the Army (reference 1a), the Department of Defense Chief Information Officer (reference 1b) and the 2015 Army Cloud Computing Strategy (reference 1c).
3. Background. As required by reference 1a, the Army must migrate enterprise-level systems and applications to hosting environments authorized by the Department of Defense (DoD) no later than the end of fiscal year (FY) 2018. This guidance provides an authorized alternative to leverage approved commercial cloud service providers to satisfy this requirement. Cloud computing is 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. Transitioning to cloud-based solutions and services advances the Army's long-term objective of reducing ownership, operation and sustainment of hardware and other commoditized information technology (IT). This transition is a critical component of the Joint Information Environment (JIE) objectives outlined in the DoD Chief Information Officer July 2013 memorandum (reference 1i). Over time, cloud computing will significantly boost operational efficiency, increase network security and posture the Army to adopt innovative technology more quickly at a lower cost.
4. Scope. This guidance applies to all Army organizations with systems and applications currently in use, under development or to be developed except those explicitly excluded in Enclosure 2, paragraph 1.
5. Guidance. In 2014 guidance, the Under Secretary of the Army directed that all systems and applications providing enterprise services migrate to designated Core Data Centers no later than the end of FY18. The guidance also established the Army Application Migration Business Office (AAMBO) and required that all systems and

SAIS-AOC

SUBJECT: Guidance for Migration to, and Use of, Commercial Cloud Service Providers (CSPs)

applications migrate to a DoD-approved hosting facility. This policy focuses on the commercial CSP migration and hosting option. It reinforces the overarching Army application migration process; identifies systems and applications not permitted to migrate to off-premises commercial CSPs; identifies roles and responsibilities for organizations with applications migrating to, or using, commercial CSPs; and outlines cybersecurity and commercial CSP acquisition and use requirements.

6. High-level process overview. The following provides a high-level overview of the process to migrate systems and applications to a DoD-approved commercial CSP. The full list of requirements, roles and responsibilities is outlined in Enclosure 2. System and application owners must:

a. Complete system and application rationalization and disposition. Commands are ultimately responsible for ensuring that all systems and applications within their IT portfolio are rationalized (per reference 1a).

b. For systems and applications with a disposition of "kill," terminate the system/application in accordance with the planned system and application termination period. If termination is expected after the end of FY18, a Plan of Action and Milestones (POA&M) is required. The POA&M must be signed by the appropriate application authorizing official (AO) (formerly the designated approving authority), appointed by the Army Chief Information Officer/G-6, and approved by the supporting mission area governance forum.

c. For new systems and applications, and those with a disposition of sustain or modernize, complete an Army IT cost-benefit analysis (CBA). The CBA is fully incorporated into the Army's IT investment governance process and fulfills DoD's enterprise IT standard business case analysis requirement (reference 1f).

d. Organizations with systems and applications approved for migration, continue to collaborate with AAMBO to complete migration to the approved CSP. AAMBO is the Army's single point of contact/broker office for all application migration planning and execution, regardless of the Army-approved CSP hosting option selected.

7. Required conditions for system and application hosting and migration to commercial CSPs. Several conditional dependencies impact an organization's ability to use commercial CSPs (Enclosure 2, Paragraph 2). System and application owners must assess these conditions against the impact level requirements for their system or application in the Cloud Computing Security Requirements Guide (reference 1d). These conditions must be satisfied and Risk Management Framework AO authorization obtained before migrating to a commercial CSP. AAMBO will monitor and maintain the current status of these conditions.

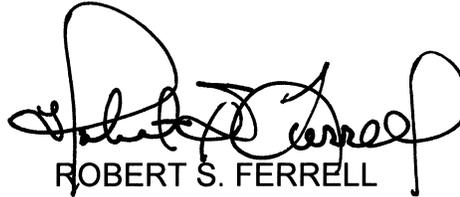
SAIS-AOC

SUBJECT: Guidance for Migration to, and Use of, Commercial Cloud Service Providers (CSPs)

8. For further information on application migration, contact AAMBO via email at usarmy.belvoir.peo-eis.mbx.army-app-migration-office@mail.mil, or Product Director Enterprise Computing, Mr. Archie Mackie, at archie.mackie.civ@mail.mil or (703) 704-2796.

9. Enforcement of this policy is effective upon the date of signature by the Chief Information Officer/G-6. This policy will be reviewed for update one year from the date of signature unless superseded earlier.

10. The points of contact for this action are: LTC Bennett Hayth, (703) 693-9905 or bennett.e.hayth.mil@mail.mil; and Mr. A.J. Bognar, (703) 697-7615 or attila.j.bognar.civ@mail.mil.



ROBERT S. FERRELL
Lieutenant General, GS
Chief Information Officer/G-6

Encls

DISTRIBUTION:

Principal Officials of Headquarters, Department of the Army
Commander

- U.S. Army Forces Command
- U.S. Army Training and Doctrine Command
- U.S. Army Materiel Command
- U.S. Army Pacific
- U.S. Army Europe
- U.S. Army Central
- U.S. Army North
- U.S. Army South
- U.S. Army Africa/Southern European Task Force
- U.S. Army Special Operations Command
- Military Surface Deployment and Distribution Command
- U.S. Army Space and Missile Defense Command/Army Forces Strategic Command
- U.S. Army Medical Command
- U.S. Army Intelligence and Security Command

SAIS-AOC

SUBJECT: Guidance for Migration to, and Use of, Commercial Cloud Service Providers (CSPs)

DISTRIBUTION: (CONT)

Commander

U.S. Army Criminal Investigation Command

U.S. Army Corps of Engineers

U.S. Army Military District of Washington

U.S. Army Test and Evaluation Command

U.S. Army Installation Management Command

U.S. Army Reserve Command

U.S. Army Accessions Support Brigade

U.S. Army Cyber Command/Second Army

Superintendent, United States Military Academy

Commandant, U.S. Army War College

CF:

Chief, Army Reserve

Director, Army National Guard

Director of Business Transformation

Commander, Eighth Army

Guidance for Migration to, and Use of, Commercial Cloud Service Providers

Enclosure 1 – References

Note: All references below are available at the Army CIO/G-6 CAC-enabled portal:
https://army.deps.mil/army/cmds/hqda_ciog6_Project/ADCCP/CloudDocRepository/

- a. Memorandum, Under Secretary of the Army, subject: Migration of Army Enterprise Systems/Applications to Core Data Centers, 9 June 2014.
- b. Memorandum, Department of Defense Chief Information Officer, subject: Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services, 15 December 2014.
- c. Army Cloud Computing Strategy, HQDA Chief Information Officer/G-6, Version 1.0, 26 March 2015.
- d. Cloud Computing Security Requirements Guide, Version 1, Release 1, 12 January 2015.
- e. Memorandum, Under Secretary of the Army, subject: The Army Business Management Strategy, 3 December 2013.
- f. Memorandum, Department of Defense Chief Information Officer, subject: Use of Enterprise Information Technology Standard Business Case Analysis, 23 October 2014.
- g. Army Regulation 381-10, U.S. Army Intelligence Activities, 3 May 2007.
- h. Memorandum, Deputy Chief of Staff, G-2, subject: Army Request for Information Technology-Military Intelligence (ARFIT-MI) Implementation Plan, 10 June 2013.
- i. Memorandum, Department of Defense Chief Information Officer, subject: Department of Defense Joint Information Environment (JIE): Continental United States Core Data Centers and System and Application Owners Migration, 11 July 2013.
- j. Federal Acquisition Regulation Supplement, Volume 1, Part 2 – Definition of Words and Terms, Subpart 2.101 – Definitions, Revised 2 March 2015.
- k. Department of Defense Instruction 8320.02, Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense, 5 August 2013.
- l. Army Regulation 25-1, Army Information Technology, 25 July 2013.
- m. National Institute of Standards and Technology Special Publication 800-82, Guide to Industrial Controls Systems Security, June 2011.

Guidance for Migration to, and Use of, Commercial Cloud Service Providers

Enclosure 1 – References

- n. Army Regulation 25-400-2, The Army Records Information Management Information System (ARIMS), 2 October 2007.
- o. Memorandum, Army Chief Information Officer/G-6, subject: Department of the Army Strategy for the Implementation of the Risk Management Framework (RMF) for Department of Defense Information Technology (IT), 12 February 2015

Guidance for Migration to, and Use of, Commercial Cloud Service Providers

Enclosure 2 - Requirements To Migrate to Commercial Cloud Service Providers

1. Systems and applications excluded from off-premises commercial cloud service providers (CSPs). The following systems and applications are not permitted to migrate to or use off-premises commercial CSPs and will continue to follow existing guidance for those systems and applications.

a. Systems that are designated as critical Military Intelligence or cryptological systems, and Army Intelligence Components, as defined in Army Regulation 381-10, will continue to follow guidance outlined in the Army Request for Information Technology-Military Intelligence Implementation Plan (reference 1h).

b. Weapon systems, mission command command-and-control systems, U.S. Army foreign military sales information technology systems (Title 22), and applications hosted solely in tactical/mobile facilities.

c. Installation-based industrial control systems (ICS), platform information technology (PIT), and supervisory control and data acquisition systems (SCADA), as defined in NIST 800-82 (reference 1m). ICS, PIT and SCADA systems include a variety of systems and mechanisms used to monitor and/or operate critical infrastructure elements that require on-site presence, such as electricity, water, natural gas, fuels, entry and access, heating and air conditioning, runway lighting, etc.

d. The U.S. Army Medical Command (MEDCOM) will continue to follow Military Health Systems procedures; its enterprise applications are excluded from this policy.

2. Enterprise Resource Planning Systems (ERPs). Army major enterprise resource planning (ERP) and key ERP-enabling systems are not permitted to migrate to or use off-premises commercial CSPs and must be migrated to a DISA Defense Enterprise Computing Center (DECC) by the end of FY18. These systems include:

- a. General Fund Enterprise Business System (GFEBS).
- b. Global Combat Support System - Army (GCSS-Army).
- c. Logistics Modernization Program (LMP).
- d. Integrated Personnel and Pay System - Army (IPPS-A).
- e. Army Enterprise Systems Integration Program (AESIP).
- f. Logistics Information Warehouse (LIW).

Guidance for Migration to, and Use of, Commercial Cloud Service Providers

Enclosure 2 - Requirements To Migrate to Commercial Cloud Service Providers

3. Required Conditions for Migration to, and Use, of Commercial CSPs. The conditional dependencies identified below will impact Army organizations' ability to migrate to and use commercial CSPs. System and application owners must assess these conditions against the impact level requirements for their system or application, and these conditions must be satisfied before systems and applications are permitted to migrate to or use CSPs. Each condition is mandatory and required to be met, unless waived by the Army CIO/G-6. AAMBO will monitor and maintain the current status of these conditions:

a. Army Cloud Hosting Contract Vehicle (ACHCV). Army organizations migrating to, or using, commercial CSPs are required to utilize the AAMBO-provided cloud contract vehicle and contracting language, or other Army-approved cloud contracting vehicles and AAMBO-provided contracting language. The Army Cloud Hosting Contract Vehicle (ACHCV) is tentatively scheduled for completion on or about 1Q FY17. The estimated contract award timeline of 12-15 months includes contract review, approval, RFP, source selection, and award. AAMBO has identified several federal contract alternatives that can potentially be used until a fully-compliant Army contract can be awarded, if all other required Application migration conditions are satisfied.

b. The commercial CSP must have a DoD Provisional Authorization (PA) and the authorization from the Army-appointed authorizing official. System and application owners must ensure that the commercial CSP is certified commensurate with the impact level of the data being hosted.

c. A DISA or DoD-approved cloud access point (CAP) is operational and available for use when using off-premise Cloud Service Providers (if required, based on impact level). The DISA CAP and CAP Security extensions are both tentatively scheduled to become operational NLT 2Q FY16, and achieve Full Operational Capability by NLT 3Q FY16.

d. Computer Network Defense Service Provider (CNDSP) requirements, commensurate with the impact level of data being hosted, are validated, approved and published by Army Cyber Command (ARCYBER), and are included in the contract language. The Army Cloud CND CONOPS is under development and tentatively scheduled to be finalized NLT end of 1Q FY16. The first draft was released for socialization on 8 July 2015 and is currently in limited-staffing.

e. Cloud-based common services must be clearly identified and provisioned and, if provided by a commercial CSP, addressed in the service level agreement within the contract/executed task order. The development of the Directory Services common services, which includes identity management and CAC/PKI, for Impact level 4/5 applications, is underway and tentatively scheduled to be available on or about NLT 1Q FY16. ARCYBER/Second Army is the Army Lead.

Guidance for Migration to, and Use of, Commercial Cloud Service Providers

Enclosure 2 - Requirements To Migrate to Commercial Cloud Service Providers

f. Cybersecurity requirements are met and required AO authorizations obtained. The system/application owner cybersecurity requirements and the AO authorization process has not changed for implementation of commercial CSOs, and is as outlined in paragraph 5 – Commercial CSP Hosting requirements and paragraph 6 - Army Organizational Responsibilities, in this enclosure. The current list of Authorizing Officials (formerly Designated Approval Authority – DAA) has not changed for implementation of commercial Cloud Service Offerings.

4. Cost-Benefit Analysis (CBA) Requirements and Process Flow. Certain preparatory steps are required prior to completing a CBA. Regardless of whether a system or application is new or existing, owners are required to determine/confirm their system and data impact levels, to complete rationalization and disposition, and to update their Command/operating agency's IT portfolio before migrating or deploying their systems and applications to a commercial CSP.

a. Impact Level Determination. System and application owners, in conjunction with their assigned AO, must determine/confirm the appropriate security, data and mission impact levels of their systems and applications prior to migration. Impact levels and security objectives are defined in the DoD Cloud Computing Security Requirements Guide.

b. Rationalization and Disposition Determination. All Army system and application owners, in conjunction with their Command/operating agency portfolio manager, are required to complete rationalization of their systems and applications to determine their disposition (kill, modernize or sustain) prior to migration. The cost of application migration will be borne by the owning Command, as stated in the 9 June 2014 Under Secretary of the Army memorandum (reference 1a). An overview of the rationalization and disposition process also is outlined in this memo.

1) For systems and applications with a disposition of kill: The system or application must be terminated no later than the end of FY18. If the projected termination period is after the end of FY18, the system/application owner, in conjunction with the Command/operating agency portfolio manager, must submit a Plan of Action and Milestones (POA&M), signed by the Army CIO/G-6-appointed system or application AO and approved by the supporting mission area governance forum (as outlined in reference 1a).

2) For new systems and applications and those with a disposition of sustain or modernize: System and application owners must take all necessary steps to ensure that their systems and applications are modernized and assessed for cloud suitability in accordance with the system and application modernization checklist described in reference 1a. A CBA must be developed to assess system and application migration hosting options.

Guidance for Migration to, and Use of, Commercial Cloud Service Providers

Enclosure 2 - Requirements To Migrate to Commercial Cloud Service Providers

c. **CBA Development.** The CBA is a core requirement for migration to any DoD-approved hosting environment. The CBA incorporates the DoD IT business case analysis guidance and provides a standardized approach and criteria for analyzing IT investments. The CBA will ensure consistency, facilitate comparisons of proposed alternatives, and clearly define expected costs, benefits, operational impacts and risks.

1) System and application owners with a disposition of sustain or modernize must follow the approved AAMBO application migration process. System and application owners must contact AAMBO and provide their system and application information in order for AAMBO to provide the System/Application Migration Assessment Report (SAMAR) needed to complete the CBA.

2) Specific Army IT investment CBA guidance is under development (by the CIO/G-6 Policy and Resources Directorate in collaboration with the Deputy Assistant Secretary of the Army - Cost and Economics) and will be published under a separate guidance memorandum, currently scheduled for completion NLT 2Q, FY16. Application bundling, where several applications could be the subject of a single CBA, will be supported in accordance with the forthcoming Army IT investment CBA guidance.

3) Army organizations must include at least one Defense Information Systems Agency hosting option, at least one commercial CSP hosting option and any other hosting options being considered in the CBA.

d. **Governance and CBA Review Process.** Commands (and operating agencies for organizations without a parent command) remain responsible for ensuring that all systems and applications in their portfolio are entered into the Army Portfolio Management Solution (APMS). Commands and operating agencies will provide a consolidated list of the results of rationalization (i.e., a kill, sustain or modernize disposition) for all systems and applications within their portfolio to the supporting domain and mission area governance forum for their mission area. This will allow the domain and mission area governance forum to determine if duplicate applications or functions exist across the domain and mission area, to eliminate inefficiencies and to enhance overall fiscal accountability within each mission area.

1) The Mission Area Governance forums are responsible for providing the endorsed list of applications to the Army CIO/G-6 (SAIS-PR) for review. Defense Business Systems owners will continue to follow Business Enterprise Architecture and Business Systems Architecture (BSA) guidelines regarding portfolio management (including binning, rationalization and disposition) in accordance with the Army Business Management Strategy (Ref 1.e). The mission area governance forums are listed below:

(a) The Army Business Council (ABC) is the three-star governance forum with oversight of defense business systems (DBS) and applications within the Business

Guidance for Migration to, and Use of, Commercial Cloud Service Providers

Enclosure 2 - Requirements To Migrate to Commercial Cloud Service Providers

Mission Area (BMA). BMA rationalization will also be captured in the Enterprise Knowledge Repository (EKR) for decision support, if available.

(b) The Army Enterprise Network Council (AENC) is the three-star governance forum with oversight of systems and applications within the Enterprise Information Environment Mission Area (EIEMA).

(c) The LandWarNet/Mission Command General Officer Steering Committee (LWN/MC GOSC) is the three-star governance forum with oversight of systems and applications within the Warfighter Mission Area (WMA).

2) Commands are required to continually review and update their portfolios in coordination with the appropriate mission areas and their subordinate domain governance forum.

3) Upon Army CIO/G-6 approval of the CBA, an "approved for migration" list will be forwarded to the appropriate governance forum, the system or application Command or operating agency, and AAMBO.

4) System and application owners whose systems and applications are on the "approved for migration" list will coordinate directly with AAMBO to continue the application migration process. System and application owners whose systems and applications are not approved for migration will be notified and re-directed to their respective command, domain or operating agency.

5. Commercial CSP Hosting Requirements.

a. Army organizations considering using commercial CSPs may only use those CSPs that host data in clouds that are within the United States or its outlying areas, as defined in FAR 2.101 (reference 1j); or in OCONUS locations that are within U.S. control and not subject to host-nation or regional laws via treaty or other circumstance. The intent is to ensure that Army files and records are subject to U.S. law, not host-nation or regional laws of a foreign country.

b. DISA retains responsibility for evaluating CSPs that are interested in hosting DoD information and for determining whether the provider meets the requirements for hosting data. DISA will evaluate the CSP offering against the requirements in the DoD Cloud Computing Security Requirements Guide and issue a DoD Provisional Authorization (PA) that describes the types of information that can be hosted in that particular CSP offering and the vulnerabilities associated with that offering. The PA is provisional; the Army AO must decide whether to allow the use of the specific CSP offering to support particular Army hosting requirements.

Guidance for Migration to, and Use of, Commercial Cloud Service Providers

Enclosure 2 - Requirements To Migrate to Commercial Cloud Service Providers

c. Army organizations may only consider the use of CSP offerings that have an approved DoD PA and the Army-specific authorization. The capability AO will ensure that the selected commercial CSP offering is on an Army cloud hosting contract vehicle (ACHCV) or other Army-approved cloud contract vehicle, and has received the appropriate PA and Army authorization for the impact level required for hosting. System and application owners are responsible for ensuring that the CSP offering meets the protection requirements for their capability. The capability AO is responsible for issuing the authorization for operations using the selected CSP offering. System and application owners may contact AAMBO for a list of authorized CSPs. Once authorized by the capability AO, an Authority to Connect (ATC) must be obtained from the ARCYBER/Second Army AO prior to migrating to the commercial CSP.

d. For non-controlled unclassified information (unclassified DoD information that has been authorized for public release), Army organizations may host those systems and applications on a commercial CSP offering that has obtained a DoD PA and Army authorization. System and application owners are responsible for ensuring that the CSP offering meets the protection requirements for their capability. The capability AO is responsible for issuing the authorization for operations using the selected CSP offering. The Cloud Security Guide (reference 1b) outlines the minimum security baseline for all security controls commercial CSPs are required to maintain.

e. For controlled unclassified information (CUI), Army organizations must connect to the commercial CSP through a DoD-approved CAP.

6. Army Organizational Responsibilities.

a. Army Application Migration Business Office (AAMBO).

1) The Under Secretary of the Army established AAMBO as the Army's single point of contact/broker office for all application migration planning and execution. AAMBO will assist system and application owners with defining technical requirements, preparing hosting cost comparisons for incorporation into the CBA, right-sizing their application hosting requirements, recommending cost-effective hosting and support strategies, and guiding system and application owners through the migration process to the commercial cloud or any other DoD-approved hosting environment.

2) AAMBO, in collaboration with the appropriate functional organizations, will develop, maintain and provide the required contracting language to be incorporated into all commercial cloud services contract vehicles and performance service level agreements, in accordance with Army and DoD policy. All Army organizations migrating systems and applications to commercial CSPs are required to use the AAMBO-provided contracting vehicle and contracting language (or other Army-approved cloud contracting vehicle and contracting language).

Guidance for Migration to, and Use of, Commercial Cloud Service Providers

Enclosure 2 - Requirements To Migrate to Commercial Cloud Service Providers

3) AAMBO will monitor and maintain the current status of commercial CSPs approved for Army use and the status of any other items approved for inclusion in the Army cloud contract vehicle, including cloud-based common services provisioning, CNDSP requirements, and DISA/DoD CAP establishment and approval.

4) AAMBO services will be centrally funded by the Army; however, resources required to perform the actual migration and subsequent hosting of the application are the responsibility of the Command or operating agency that owns the system or application.

b. Army CIO/G-6 Cybersecurity.

1) On 12 February 2015, the Army CIO/G-6 published the Department of the Army Strategy for Implementation of the Risk Management Framework (RMF) for Department of Defense Information Technology (IT) (reference 1o). The RMF establishes cybersecurity policy and assigns responsibility for executing and maintaining the RMF. It applies to all Army IT that receives, processes, stores, displays and/or transmits DoD/Army information. The Army CIO/G-6 is responsible for overall administration of the RMF and remains the Army authorizing official.

2) Army organizations are required to transition to the RMF per the timelines established by the Army CIO/G-6 Implementation of the RMF memo.

3) Army CIO/G-6 Cybersecurity will collaborate with AAMBO on frequently updated cybersecurity information, including information regarding any commercial CSPs that have received or lost Army authorization, DISA/DoD-approved CAP provisioning, and changes in Army cybersecurity risk management procedures.

c. U.S. Army Cyber Command (ARCYBER).

1) ARCYBER serves as the computer network defense service provider (CNDSP) for the Army. The CNDSP mission requires integrating, implementing and conducting network defense, including actions necessary to protect, monitor and sustain all Army networks. ARCYBER will detect, analyze and respond to all threats by directing the use of dynamic forensics and the employment of appropriate cyber forces. ARCYBER forces must be enabled to navigate within the commercial CSP cloud environment when required to perform its CNDSP role.

2) ARCYBER will collaborate with AAMBO to provide CNDSP requirements, commensurate with impact levels, to govern CSP performance. These requirements will be included in the ACHCV and service level agreement, and in Army-approved and/or AAMBO-provided cloud computing contract language.

Guidance for Migration to, and Use of, Commercial Cloud Service Providers

Enclosure 2 - Requirements To Migrate to Commercial Cloud Service Providers

3) Successful operation and defense require collaboration and information sharing among all Army and DoD organizations, including DISA/DoD CNDSP, ARCYBER, Army National Guard and the commercial CSP. ARCYBER will collaborate with all Army internal and external CNDSP partners as necessary to perform its Army CNDSP mission.

d. Army Command/Operating Agencies, System and Application Owner Responsibilities.

1) Preparation for migration to the cloud computing environment. For systems and applications identified for migration to the cloud computing environment, system and application owners must coordinate with AAMBO to analyze and right-size their application hosting requirements, thereby ensuring that the Army buys only what is needed (and avoids moving to the cloud environment with over-provisioned capacity requirements). System and application owners must collect performance data to support this level of engineering analysis. AAMBO will assist Commands with the system planning required to move applications to the cloud.

2) The Army organization requesting migration to a commercial CSP is responsible for determining which data and missions may be hosted on a commercial cloud, and must ensure that the migrated system/application remains compliant with all Army directives, policies and privacy, legal and regulatory considerations. System and application owners, in coordination with AO appointed by the Army CIO/G-6, must also evaluate mission risk with respect to information compromise, loss of integrity, confidentiality and/or availability, as well as the impact of any compromise or loss. Army organizations must obtain all Army-required AO authorizations prior to operating in a commercial CSP.

Additionally, owners must ensure that their cloud-hosted systems and applications are properly registered with DISA through the Systems/Networks Approval Process (SNAP) Cloud Module (<https://snap.dod.mil/gcap/home.do?sys=CLD>).

3) Army organizations acquiring or using commercial cloud services are responsible for ensuring that the contract language fully addresses their system, application and storage requirements. Army organizations, in coordination with their assigned AO, must coordinate with ARCYBER to ensure that cyber defense of information and mission data, and all end-to-end security requirements, are fulfilled and maintained.

4) Army organizations must capture performance metrics for applications that have migrated to commercial CSPs. Additional details of the information frequency, format, timing, measures and targets used to assess performance will be outlined in the next update of this policy document.

Guidance for Migration to, and Use of, Commercial Cloud Service Providers

Enclosure 2 - Requirements To Migrate to Commercial Cloud Service Providers

5) Commands are responsible for funding application migration and hosting, in accordance with reference 1a. In order to ensure resourcing availability, commands, portfolio managers, and system and application owners must conform with the following resourcing imperatives (as applicable).

(a) Use existing hardware refresh or major software upgrade resourcing to cover costs.

(b) Perform rationalization with an emphasis on killing duplicative systems, thereby providing greater flexibility in funding retained applications.

(c) Identify any additional resource gaps and perform internal Command resource prioritization before engaging the Army Budget Office or G-8 for additional resource support.

(d) Ensure compliance with the Program Budget Assessment Team (PBAT) review guidelines.

(e) Provide key artifacts (e.g., AAMBO artifacts, Milestone 1 initial enduring data center rough order of magnitude and work breakdown structure, Milestone 5 cost estimate, Milestone 6 migration plan) to the Command resource manager, MDEP manager, PEG Panel and PBAT for resourcing validation. (See reference 1a.)

(f) Conduct contract coordination within the Command. A Command approach to application migration is encouraged to ensure that existing contracts are checked and coordinated when moving to an enterprise environment.

(g) Ensure compliance with data-sharing requirements. All Army organizations transitioning to a commercial CSP must ensure that IT services and data identified for transition are compliant with DoD Instruction 8320.02, Sharing Data, Information, and Information Technology Services in the DoD (reference 1.k) and, AR 25-1, Army Information Technology (reference 1.l), before the transition is completed.

(1) All IT capabilities and content hosted in a cloud will be visible, accessible, understandable, trusted and interoperable.

(2) Data sources transitioning to the cloud must be registered and approved as an Authoritative Data Source (ADS) in the DoD Data Services Environment (DSE). The DSE contains the structural and semantic metadata artifacts critical to successful development, operation, and maintenance of existing and future capabilities that support the DoD Net-Centric Data Strategy. The DSE serves as a key enabler to make data "visible, accessible, and understandable" by implementing it as an Enterprise

Guidance for Migration to, and Use of, Commercial Cloud Service Providers

Enclosure 2 - Requirements To Migrate to Commercial Cloud Service Providers

service; Streamlining search and access for data; and providing a set of tools to register and discover data services across the DoD.

(3) An Authoritative Data Source is a recognized or official data production source with a designated mission statement or source/product to publish reliable and accurate data for subsequent use by customers. An authoritative data source may be the functional combination of multiple, separate data sources, and consist of three items: Data Need; System, and a Data Producer. Authoritative Data Elements are Data Elements that the System and Data Producer owns, produces, controls and stores.

(4) All IT capabilities and content hosted in the cloud must adhere to standards in the DoD IT Standards Registry or to the standards specified in the applicable Army Common Operating Environment Standard View.

6) Army Records Management Requirements. All Army organizations transitioning to and or using a commercial CSP must continue to comply with the Department of the Army Records Information Management System (ARIMS) program for retention and records management, per AR 25-400-2.

(a) ARIMS applies to all unclassified Army record information, including For Official Use Only (FOUO), regardless of format or medium (paper, electronic (electronic mail (e-mail), information system data files/databases, word processing, bit-mapped), microfilm, etc.).

(b) ARIMS does not apply to:

(1) Record copies of international agreements covered under AR 550-51 (except those maintained by the Office of the Judge Advocate General).

(2) Publications and blank forms stocked for filling requisitions.

(3) Reference materials and books in formally organized and officially designated libraries.

(4) Personal or private records maintained in the workplace.

(5) Duplicate copies of documents maintained in the same file.

Guidance for Migration to, and Use of, Commercial Cloud Service Providers

Enclosure 2 - Requirements To Migrate to Commercial Cloud Service Providers

7. Waivers.

a. Existing Contract Waiver. System and application owners who have a signed commercial CSP contract, or will sign a contract within 45 days of the signing of this policy memorandum, are allowed to maintain the existing contract but are required to:

1) Contact AAMBO and provide their system and application information. System and application owners must also provide the Army CIO/G-6 (SAIS-AOC) and the appropriate mission area governance forum a copy of the contract within 45 days of approval of this policy memorandum. This will allow the mission area governance forum to review the current level of risk being accepted and determine whether it is in compliance with the Army cloud computing guidelines outlined in this policy.

2) Prior to executing follow-on option years of or renewing the contract, system and application owners must contact AAMBO, complete an application review and CBA, and provide them to AAMBO and the appropriate mission area governance forum.

b. Unanticipated or undocumented cases that require a waiver will be reviewed on a case-by-case basis by the mission area and supporting domain governance forums, then forwarded to the Army CIO/G-6 Policy and Resources Directorate for review and decision.