SECRETARY OF THE ARMY
WASHINGTON

09 DEC 2016

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Army Directive 2016-38 (Migration of Army Systems and Applications to Approved Hosting Environments and Consolidation of Data Centers)

1. References. A complete list of references is at enclosure 1.

2. This directive establishes an implementation plan (enclosure 2) for a range of actions necessary for the Army to rationalize and modernize information technology (IT) systems and applications, migrate them to approved hosting environments (enclosure 3), and close or consolidate data centers (enclosure 4).

3. The Chief Information Officer (CIO)/G-6 governs implementation of this plan through the Army Enterprise Network Council (AENC) using the Migration Implementation and Review Council as its advisory body (defined in enclosure 2). AENC will provide quarterly updates to the Senior Review Group beginning no later than 120 days after the date of this directive.

4. This directive applies to all Army systems and applications currently in use or under development and to all future developments except those specifically excluded in enclosure 5. Reference a is hereby rescinded.

5. During fiscal year 2015 (FY 15), the Army spent $8.3 billion on a wide range of IT products and services, including IT systems, applications, manpower, and host facilities. Many of these systems and applications are necessary for efficient operations; many are not. In addition, our systems and networks are under constant threat of compromise and disruption. Every IT system and application presents a potential attack surface to those wishing to affect our readiness to respond when required. We can no longer afford the luxury of unconstrained IT expenses nor accept the risk to the Army and the Nation posed by cyber threats directed against Army capabilities.

6. On 9 June 2014, the Under Secretary of the Army issued guidance to establish the Army Application Migration Business Office and outlined a process for migrating enterprise systems to core data centers (reference a). In the interim, the Department of Defense (DoD) CIO and the Army CIO/G-6 issued additional clarifying guidance (references b–d). However, progress in system and application virtualization and rationalization has been slow, and our data center closure and consolidation efforts have come to a virtual standstill. Additionally, in February 2016, the Deputy Secretary of Defense directed DoD to complete a rapid deployment and transition to Microsoft Windows 10 because of the need to strengthen our cybersecurity posture while

concurrently streamlining the IT operating environment (reference x). I therefore direct the following:

a. Implementation of the enclosed revised plan for migrating systems and applications and consolidating data centers.

b. Closure of installation processing nodes identified in enclosure 4, table 2, as well as the closure of any additional nodes, as required, not identified (including data centers under Army proponency).

c. Assessment of the feasibility, suitability, and acceptability for closing special purpose processing nodes identified in enclosure 4, table 2 through a collaborative effort between affected Army Commands and the Migration Implementation and Review Council, to include identifying special purpose processing nodes requiring exemption from closure.

d. Army Commands will complete the transition to Microsoft Windows 10 no later than 31 January 2017. Organizations unable to meet that suspense date may request a waiver through the appropriate process the Army CIO/G-6 and DoD have established.

7. Your direct leadership is required to ensure that implementation of this plan produces the desired strategic effects of streamlining our IT portfolios, saving corresponding resources that can be applied toward Army requirements, shrinking our data center footprint, and reducing cyber threats to our networks.

8. This directive will remain in effect until it is rescinded.

Encls

Eric K. Fanning

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
(CONT)

DISTRIBUTION: (CONT)
- 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 Strategic Command
- U.S. Army Cyber Command
- U.S. Army Medical Command
- U.S. Army Intelligence and Security Command
- 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
- Second Army

Superintendent, United States Military Academy
Director, U.S. Army Acquisition Support Center
Executive Director, Arlington National Cemetery
Commandant, U.S. Army War College
Commander, U.S. Army Accessions Support Brigade

CF:
Director, Army National Guard
Director of Business Transformation
Commander, Eighth Army

REFERENCES

a. Memorandum, Under Secretary of the Army, 9 June 2014, subject: Migration of Army Enterprise Systems/Applications to Core Data Centers (hereby rescinded).

b. Memorandum, Department of Defense (DoD) Chief Information Officer (CIO), Oct 23, 2014, subject: Use of Enterprise Information Technology Standard Business Case Analysis.

c. Memorandum, DoD CIO, Dec 15, 2014, subject: Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services.

d. Memorandum, SAIS-AOC, 23 July 2015, subject: Guidance for Migration to, and Use, of Commercial Cloud Services Providers (CSPs).

e. Memorandum, DoD CIO, Jul 11 2013, subject: Department of Defense Joint Information Environment: Continental United States Core Data Centers and Application and System Migration.

f. Deputy Assistant Secretary of the Army for Cost and Economics Cost-Benefit Analysis (CBA) Guide, 3rd Edition (v3.10), 24 April, 2013.

g. Army Cloud Computing Strategy, Version 1.0, 26 March 2015.

h. DoD Cloud Computing Security Requirements Guide, Version 1, Release 2, 18 March 2016.

i. Department of the Army Pamphlet 25-1-1 (Army Information Technology Implementation Instructions), 26 September 2014.

j. Memorandum, SAIS-CBA, 27 Apr 2012, subject: Disposal of Excess Information Technology Equipment - Leased IT Equipment.

k. Memorandum, SAIS-PRI, 14 Aug 2013, subject: Approvals/Waivers for Obligation of Funds for Data Servers and Centers Information Technology (IT) Spending.

l. Memorandum, Deputy Chief of Staff, G-2, 10 Jun 2013, subject: Army Request for Information Technology-Military Intelligence (ARFIT-MI) Implementation Plan.

m. National Institute of Standards and Technology (NIST) Special Publication 800-82 (Guide to Industrial Controls Systems Security), June 2011.

n. Memorandum, SAIS-CB, 12 Feb 2015, subject: Department of the Army Strategy for the Implementation of the Risk Management Framework (RMF) for Department of Defense Information Technology (IT).

o. DoD Instruction 8320.02 (Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense), August 5, 2013.

p. Army Regulation (AR) 25-1 (Army Information Technology), 25 June 2013.

q. AR 25-400-2 (The Army Records Information Management System) (ARIMS), 2 October 2007.

r. Memorandum, Under Secretary of the Army, 3 Dec 2013, subject: The Army Business Management Strategy.

s. All Army Activities (ALARACT) 045/2015 - MOD 2 to HQDA Execute Order 209-11, Army Data Center Consolidation Plan, 05 March 2013.

t. NIST Special Publication 800-145 (The NIST Definition of Cloud Computing), September 2011.

u. Army Doctrine Publication 6-0 (Mission Command), 17 May 2012.

v. NIST Special Publication 800-146 (Cloud Computing Synopsis and Recommendations), May 2011.

w. Federal Acquisition Regulation Supplement, Volume 1, Part 2 (Definition of Words and Terms), Subpart 2.101 (Definitions), Revised 2 March 2015.

x. Memorandum, Deputy Secretary of Defense, Feb 26, 2016, subject: Implementation of Microsoft Windows 10 Secure Host Baseline.

y. Instruction, Committee on National Security Systems (CNSS), 6 April 2015, subject: Glossary.

z. Title 22, United States Code, Chapter 39, Sub Chapter II – Foreign Military Sales, Section 2761, 18 December 2014.

IMPLEMENTATION PLAN FOR SYSTEM AND APPLICATION RATIONALIZATION AND MIGRATION

1. References. A complete list of references is in enclosure 1.

2. Purpose. This implementation plan establishes and directs a range of actions necessary for the Army to rationalize and modernize information technology (IT) systems and applications and migrate them to approved hosting environments.

3. Scope. This plan is applicable to all Army IT systems and applications regardless of command or proponent (hereafter referred to as Army commands), domain, or mission area, except those specifically exempted in enclosure 5.

4. Intent of the Secretary of the Army and Chief of Staff, Army. Our IT system and application rationalization and migration effort aims to accomplish three major objectives:

a. Reduce the number of Army IT systems and applications and optimize those remaining to operate in modern, cloud-enabled computing environments. We can no longer afford unconstrained IT spending nor embrace local IT hosting solutions apart from our desired enterprise approach.

b. Realize that cyber-related threats to our systems, applications, and networks pose significant risks to our ability to generate and sustain ready forces; protect the unit and personal information of our formations, Soldiers, and Family members; and secure our installations and activities. We can no longer underwrite these risks or tolerate antiquated IT software, hardware, and policies that present potential attack surfaces for exploitation.

c. Reduce our IT hosting-related costs by establishing and adhering to authorized network and hosting capabilities at each Army installation and command and by hosting every enterprise-level system and application in facilities capable of providing first-class service while reducing vulnerabilities and potentially saving resources.

5. Application Migration and Data Center Consolidation Strategy. To achieve these three major objectives, the Chief Information Officer (CIO)/G-6 published a comprehensive set of strategies and policies that provide the requisite foundation for action. Army commands and activities will aggressively execute those strategies and adhere to those policies within available resources.

a. Objective End State. The end state includes all enterprise systems and applications being approved, planned, resourced, and migrated to enterprise hosting environments no later than 30 September 2018, contingent upon the availability of enterprise hosting environments. Army enterprise resource planning (ERP) systems, if not already migrated, are scheduled for migration to a Defense Information Systems

Agency (DISA) Defense Enterprise Computing Center (DECC) as part of the Army ERP enclave. The suspense for ERP migration, subject to availability of funds, is 30 September 2018. The Army is reducing its data center inventory to one installation processing node (IPN) for each post, camp, or station as part of the larger Department of Defense (DoD) goal to reduce data center infrastructure by at least 60 percent from the current baseline. Reducing the Army's data center inventory will enable the Army to make the follow-on transition to its long-term end state of four continental United States (CONUS) Army Enterprise Data Centers (AEDCs) and six outside the continental United States (OCONUS) AEDCs. This facilitates implementation of the Army Private Cloud - Enterprise (APC-E) in the 2025 timeframe and is consistent with the Army's Cloud Computing Strategy (reference g), which leverages approved DoD, Federal, and commercial cloud service providers (CSPs). (A complete glossary of terms is in enclosure 6.)

b. Measures of Success

(1) No later than 180 days from the date of this directive, achieve complete application rationalization and disposition decision through the mission area level (modernize, sustain, or terminate) of all applicable IT systems and applications, regardless of mission area.

(2) No later than 30 September 2018, only legacy systems and applications with scheduled terminations by 30 September 2020 and with approved waivers and a supporting plan of action and milestones (POA&Ms) will remain on Army networks. Waivers are contingent upon these systems and applications continuing to meet the requirements for operating on an Army network.

(3) No later than 30 September 2018, migrate all Army ERP systems to DISA DECC environments and fully establish the ERP enclave.

(4) No later than 30 September 2025, ensure that all Army commands and installations are compliant with the data center target detailed in this plan and management oversight is in place to monitor new entries to the Army data center inventory.

c. Incentives

(1) The modernization and migration of applications to virtualized environments is proven to reduce application support costs. Army commands develop business cases that create real savings through a combination of application rationalization (including elimination), modernization, and migration to approved virtualized data center environments. Army commands may use the savings they achieve to address command shortfalls during year of execution. Policy requires Army commands to reduce requirements consistent with savings they achieve in the Future Years Defense Plan.

(2) Army commands should close data centers ahead of the schedule in enclosure 4, table 2 and leverage any efficiencies earned through the closures to reinvest in other IT mission needs (such as Windows 10 migration).

(3) Organizations that accelerate migrations and data center closures that create tangible real savings are the primary beneficiaries of those savings in the year of execution contingent upon and consistent with Department of the Army budget execution guidance the Assistant Secretary of the Army (Financial Management and Comptroller) publishes. Organizations that experience savings can keep those savings in their accounts (for example, Army commands for direct applications costs).

6. Definitions. For the purposes of this plan, the following definitions are in place.

a. Rationalization. Portfolio rationalization, or portfolio management, is the systematic management of IT investments within a portfolio, which includes identifying, prioritizing, authorizing, managing, and controlling applications. The focus of the rationalization effort is to identify value-added applications capable of serving a broader Army enterprise audience and garnering efficiencies through the elimination of outdated, legacy, and duplicative applications.

b. Modernization. Applications that have been upgraded or enhanced and brought into compliance with Army Common Operating Environment standards in accordance with the modernization checklist provided by the Army Application Management Business Office (AAMBO). The ALTESS Data Center (RFAA_VA_ALT_01) is designated as a modernization hub for Army commands and is available to facilitate Army application modernization support.

c. Virtualization. The act of creating a virtual (rather than actual) instance of an object, including but not limited to, creating a virtual computer hardware platform, operating system, storage device, or computer network resource.

d. Application Rationalization Methodology. Army commands select the application rationalization methodology or tool that best fits their needs for conducting a holistic review of the application portfolio. An available Army Portfolio Rationalization Guide describes an IT asset value assessment methodology that allows Army commands to better visualize and analyze the IT assets within their portfolio, including system and application dependencies, while enabling a quicker and more comprehensive portfolio management decision process. Army commands complete rationalization at the command, domain, and mission area levels and certify rationalizations by submitting a memorandum signed by the first general officer/member of the Senior Executive Service within the chain of command.

e. Hosting Solutions at Data Centers and Processing Nodes

(1) Army Enterprise Data Center. An AEDC is a fixed Army data center that provides high-capacity network infrastructure, security, technology, and operations.

AEDCs are a unique category of IPNs because they can host both local and enterprise applications. The Army intends to establish 10 AEDCs: 4 in CONUS located at Fort Bragg, NC (FBRG_NC_NEC_04); Fort Carson, CO (FCRS_CO_NEC_01); Fort Knox, KY (FKNX_KY_HG1_01); and Redstone Arsenal, AL (RDST_AL_NEC_01); and 6 OCONUS locations to be determined. AEDCs either collocate with or connect to a joint regional security stack as they come online, in accordance with Joint Information Environment (JIE) requirements. In the interim, top-level architecture stacks will continue to provide network security. To ensure consistency in operations and maintenance, service provisioning and costing, ownership and operation of each IPN designated as an AEDC will be transitioned to Second Army. Transition of the AEDCs at the Headquarters, Department of the Army (HQDA) Deputy Chief of Staff, G-1 (U.S. Army Human Resources Command (HRC)) IPN at Fort Knox and the U.S. Army Forces Command (FORSCOM)/U.S. Army Reserve Command (USARC) IPNs at Fort Bragg to Second Army will take place based on the outcome of an event-driven cost-benefit analysis (CBA).

(2) Tactical Processing Node. Tactical/mobile processing nodes provide networked services to the tactical or deployed environment and are excluded from this policy.

(3) Installation Service Node (ISN). A facility containing the localized equipment necessary to provide the minimum basic functionality to an installation should it become disconnected from the Department of Defense Information Network (DoDIN). An ISN does not host applications or process data. Potential services include read-only Active Directory servers, Domain Name System servers, Assured Compliance Assessment Solution servers, Host-Based Security System servers, and print servers. In addition, ISNs may host unified capabilities that must remain on the installation to enable emergency services when the connection to the DoDIN is interrupted. As part of the Army's data center end state, most posts, camps, and stations will retain only an ISN.

(4) Installation Processing Node. IPNs are a fixed DoD data center providing local services to a single DoD installation and local area (installations physically or logically behind the network boundary). An IPN has all of the capabilities of an ISN plus the ability to process and store local applications (that is, applications that do not cross two or more installations).

(5) Special Purpose Processing Node. SPPNs are a fixed data center, or data servers in a fixed facility, supporting special purpose functions that cannot or should not be supported by IPNs because of their association with mission-specific infrastructure or equipment. Examples are meteorology; medical; modeling and simulation; test ranges; classrooms; and research, development, test, and evaluation.

7. Plan Overview. The implementation plan consists of six steps divided into two mission-focused phases. The phased approach for migration focuses organizational efforts and aligns with the Application Migration Process Flow (enclosure 3).

These phases may run sequentially or concurrently based on the progress of individual organizational efforts.

a. Phase 1: Mission Planning

(1) Step 1: Discovery and Portfolio Analysis. This step begins with the system or application owner executing a complete system and application discovery, binning (assigning the system or application to a corresponding domain and mission area), rationalization, and disposition decision (kill, modernize, or sustain). Step 1 ends when the command provides the domain and mission area the portfolio rationalization results and disposition decisions. The mission area provides the approved-for-migration system and applications list to the Army CIO/G-6 and the command prepares to begin migration readiness assessments. Tasks completed during this step include IT portfolio documentation in the Army Portfolio Management Solution (APMS), IT portfolios properly binned to appropriate mission areas and domains, IT portfolios rationalized and disposition decisions rendered, waivers submitted, rationalized application portfolio finalized, the endorsed application list submitted by the mission area governance forum to the CIO/G-6, and the CIO/G-6 providing a reviewed and approved list to the AAMBO.

(2) Step 2: Migration Readiness Assessment. This step is initiated when AAMBO acknowledges receipt of the Army organization's endorsed application migration list from the Army CIO/G-6. This step ends with AAMBO providing a migration readiness assessment report (including engineering change proposal) that supports the system and application owner's completion of a total cost of ownership and a cost evaluation of the "as is" and "to be" environments. Tasks completed during this phase include verification of system and application registration in APMS, system engineering analysis, all modernization activities on the AAMBO-approved modernization checklist, recommendation of the target enterprise hosting environment, rough order of magnitude cost estimate for target hosting environments, and total cost of ownership and migration cost assessments (performed by system/application owner).

(3) Step 3: Cost-Benefit Analysis. A CBA is initiated when the Army organization finishes prioritizing its migrating systems and applications, and has received the Migration Assessment Report from AAMBO. This phase ends when the Deputy Assistant Secretary of the Army (Cost and Economics) (DASA-CE), in coordination with the Army CIO/G-6, approves the CBA. Tasks completed during this step include the organization completing and submitting the CBA on the DASA-CE portal to trigger an automatic workflow notification to the domain, mission area, and Army CIO/G-6; the domain reviews the CBA and provides recommendations to the mission area; the mission area reviews and endorses the CBA; the Army CIO/G-6 reviews and provides the final endorsement of the CBA; and the DASA-CE (in coordination with the Army CIO/G-6), approves or disapproves the CBA.

(4) Step 4: Migration Planning. This step begins with the CBA approval and ends with initiation of target environment support services. Tasks completed during this phase include implementation of the migration plan, completion of the authorization

process for the risk management framework (RMF), as defined in reference n, and training (as required), completion of the statement of objective/statement of work, initiation of contracting activities, coordination of service level agreement (SLA) coordination, initiation of CSP hosting option service, and transfer of funds or execution of military interdepartmental purchase request.

b. Phase 2: Mission Execution

(1) Step 5: Migration Execution. This step begins with initiation of the RMF authorization process and, in parallel, application owner migration execution activities. This step ends after completion of migration and RMF core activities and establishment of continuous monitoring. Tasks completed during this phase include completion of RMF core activities, analysis and testing of candidate platforms, migration rollout, and cutover/go live.

(2) Step 6: Quality Assurance and Steady State. This step begins with preparation for acceptance and ends with decommissioning original equipment (in accordance with reference g) and closing the original hosting data center, if applicable. Tasks completed during this phase include quality assurance, synchronization of SLAs, client acceptance, contract acceptance, and publication of lessons learned.

c. Future State. IPNs will continue to collapse into AEDCs as the Army completes the migration of applications to enterprise hosting environments. The Army will reduce its IPN inventory to 10 AEDCs by 2025, allowing for the development and maturation of the APC-E. The APC-E will be an on-premises, commercial cloud instantiation that is contractor-owned and contractor-operated. Installations that lose IPN capabilities will retain an ISN. Army commands retain the SPPNs necessary to meet mission requirements.

d. Governance Framework. The Secretary of the Army establishes the Migration Implementation and Review Council (MIRC) chaired by the Deputy CIO/G-6 and the Deputy Chief Management Officer. The MIRC reports to the Chair, AENC. Membership includes selected representation from Army staff and commands as well as mission areas. The MIRC has the following objectives:

(1) Synchronize the implementation plan across the Army;

(2) Adjudicate and elevate requests to deviate from the implementation plan, as required;

(3) Advise and recommend changes to the implementation plan;

(4) Validate the implementation plan's data center closure list (enclosure 4, table 2) and assess the operational effects of the closures on Army commands, including consideration of CBA for alternative application hosting environments; and

(5) Report Army compliance with the implementation plan to the AENC.

Quarterly, the Chair, AENC reports implementation progress to the Senior Review Group. The CIO/G-6 Army Data Center Consolidation Plan team serves as the Secretariat and analyzes, tracks, and coordinates actions for the MIRC.

8. Tasks

a. Assistant Secretary of the Army (Acquisition, Logistics, and Technology) (ASA (ALT)) will:

(1) complete rationalization and a disposition decision of the acquisition domain IT portfolio no later than 120 days from the date of this directive. Ensure update of the resultant target environment and Systems View-8 (SV-8) and annotation of decisions in the fiscal year 2017 (FY 17) request for funds certification.

(2) manage AAMBO within the Program Executive Office Enterprise Information Systems (PEO EIS) to serve as the Army's central coordinating office for migration-related planning, preparation, and execution. Ensure that AAMBO has software engineering expertise to advise system and application owners on hosting requirements and on the best, most cost-effective migration and hosting solutions.

(3) ensure that AAMBO recommends the most cost-effective hosting and support strategies, provides the Army application migration contract vehicle (and Army-approved contracting language for other approved cloud contract vehicles), and supports system and application owners throughout the migration process.

(4) provide software engineering advice to application and system owners concerning the feasibility of hosting non-ERP systems in the DISA-DECC hosting environment.

(5) establish and monitor application migration support standards that enable organizations to perform AAMBO-like functions. These functions include providing technical assessments of systems and applications (reengineering, right-sizing, modernization, and virtualization requirements); supplying technical assessments of appropriate systems and applications enterprise hosting environments; delivering the Migration Assessment Report, which includes the rough order of magnitude costs needed to support CBA development; and facilitating the systems and applications migration process.

(6) identify, in coordination with the Army CIO/G-6 and in concert with the data center end state specified in enclosure 4, technical standards that synchronize the end state with the data center/cloud/generating force computing environment as part of the Army's Common Operating Environment.

(7) coordinate with the Army CIO/G-6 and AAMBO to complete an assessment to determine if all approved enterprise hosting environments are compliant with the data center/cloud/generating force computing environment.

(8) coordinate with the Army CIO/G-6 to develop and publish checklists and other guidance to support Armywide application migration efforts, including application modernization activities that support maturation of the data center/cloud/generating force computing environment.

b. Assistant Secretary of the Army (Financial Management and Comptroller). The Assistant Secretary will:

(1) complete rationalization of the Financial Management Domain IT portfolio no later than 120 days from the date of this directive. Make sure the resultant target environment and SV-8 are updated and decisions are annotated in the FY 17 funds certification request.

(2) migrate, in coordination with the PEO EIS and within available resources, the General Fund Enterprise Business System (GFEBS) and GFEBS-Sensitive Activities ERPs to the approved DISA-DECC ERP enclave environment no later than 30 September 2018.

c. Assistant Secretary of the Army (Installations, Energy and Environment). The Assistant Secretary will:

(1) complete rationalization of the Installations, Energy, and Environment Domain IT portfolio in coordination with the Assistant Chief of Staff for Installation Management and no later than 120 days from the date of this directive.

(2) ensure the update of the resultant target environment and SV-8 and annotation of decisions in the FY 17 funds certification request.

d. Assistant Secretary of the Army (Manpower and Reserve Affairs). The Assistant Secretary will:

(1) complete rationalization of the Human Resources Domain IT portfolio in coordination with the Deputy Chief of Staff (DCS), G-1 no later than 120 days from the date of this directive.

(2) ensure update of the resultant target environment and SV-8 and annotation of decisions in the FY 17 funds certification request.

e. General Counsel. The General Counsel will ensure the provision of appropriate legal support in conjunction with The Judge Advocate General.

f. Chief Information Officer/G-6. The CIO/G-6 will:

(1) begin the MIRC and perform Secretariat functions in support of the MIRC no later than 90 days from the date of this directive.

(2) ensure that the Office of the CIO/G-6 Enterprise License Division develops, staffs, and publishes a policy and associated procedures for centrally managing and tracking equipment and software licenses that have migrated to approved enterprise hosting environments no later than 90 days from the date of this directive. The division collaborates with DISA and Second Army, in coordination with U.S. Army Cyber Command (ARCYBER), to ensure documentation of IT hardware, software, and licenses that have been transferred to DISA or other approved enterprise hosting environments. The division ensures the appropriate transfer of ownership and responsibility for maintenance agreements, which will be included in the SLA between the Army, DISA, or other enterprise hosting organization, as appropriate. Software licenses transferred to DISA will be removed from the Army inventory, as applicable.

(3) develop performance assessment plan to assess progress toward this plan's measures of success. Brief assessments monthly through the MIRC to the AENC and quarterly to the Senior Review Group, beginning no later than 120 days from the date of this directive.

(4) fund AAMBO and establish priorities, as required, for application migration to enterprise hosting environments.

(5) develop and implement a rationalization and migration plan for all systems and applications within the Enterprise Information Environment Mission Area and complete rationalization no later than 180 days from the date of this directive. Coordinate with the Office of Business Transformation on best practices rationalization methodologies to assist with this task.

(6) integrate the tracking tool data for the Army Data Center Consolidation Plan into the APMS warehouse to create the foundation for an authoritative database to track and monitor application migration and data center closures no later than 30 June 2017.

(7) review and approve requests from organizations to perform AAMBO-like functions in lieu of AAMBO, contingent upon the organization validating that it can meet the AAMBO standards the ASA (ALT) established.

g. The Auditor General. The Auditor General will develop an audit plan for Secretary of the Army approval to measure compliance with this plan beginning in FY 17.

h. Chief, National Guard Bureau. The Chief will support mission area and respective domain leads in rationalization and migration actions involving Army National Guard (ARNG) systems and applications.

i. Deputy Chief of Staff, G-1. The DCS, G-1 will:

(1) complete rationalization of the Human Resources Domain IT portfolio in coordination with the Assistant Secretary of the Army (Manpower and Reserve Affairs) no later than 120 days from the date of this directive.

(2) ensure the update of the resultant target environment and SV-8 and annotation of decisions in the FY 17 funds certification request.

(3) coordinate with the PEO EIS to remove the Integrated Personnel and Pay System-Army (IPPS-A) production environment from AEDC, Fort Knox no later than 60 days after the successful fielding of IPPS-A increment 2.

(4) ensure that HRC completes an event-driven CBA, including developing courses of action (COAs), to determine Second Army's ability to deliver IT capabilities to HRC's customer base at or above existing service levels and at or below existing costs. HRC should complete the CBA, in concert with Second Army, no later than 120 days from the date of this directive.

j. Deputy Chief of Staff, G-2. No later than 120 days from the date of this directive, the DCS, G-2 will plan for migration to Intelligence Community and Army Data Centers and continued enduring military intelligence SPPNs in support of intelligence missions.

k. Deputy Chief of Staff, G-3/5/7. The DCS, G-3/5/7 will:

(1) complete rationalization of the Training and Readiness Domain IT portfolios within the Business Mission Area (BMA) no later than 120 days from the date of this directive.

(2) ensure the update of the resultant target environment and SV-8 and annotation of decisions in the FY 17 funds certification request.

(3) review other domain portfolios within the Warfighting Mission Area for conformity to this plan's directions.

(4) complete rationalization of and migration planning for systems and applications within the Warfighting Mission Area and migrate within existing resources no later than 180 days from the date of this directive.

l. Deputy Chief of Staff, G-4. The DCS, G-4 will:

(1) complete rationalization of the Logistics Domain IT portfolio no later than 120 days from the date of this directive.

(2) ensure the update of the resultant target environment and SV-8 and annotation of decisions in the FY 17 funds certification request.

(3) ensure, in coordination with the PEO EIS, the migration of the Global Combat Support System-Army ERP to the approved DISA DECC ERP enclave environment no later than 30 September 2018.

m. Deputy Chief of Staff, G-8. The DCS, G-8 will provide programming support as required to realize the provisions of this plan during the building of Program Objective Memorandum (POM) 19–23.

n. Chief, Army Reserve. The Chief, Army Reserve will support mission area and respective domain leads in rationalization and migration actions involving U.S. Army Reserve systems and applications.

o. Assistant Chief of Staff for Installation Management. The Assistant Chief of Staff for Installation Management will:

(1) coordinate with the Assistant Secretary of the Army (Installations, Energy and Environment) to complete rationalization of the Installations, Energy and Environment Domain IT portfolio no later than 120 days from the date of this directive.

(2) ensure the update of the resultant target environment and SV-8 and annotation of decisions in the FY 17 funds certification request.

(3) analyze whether Headquarters Army Environmental System should be hosted in the DISA DECC ERP hosting environment. Provide a recommendation to the Under Secretary of the Army through the MIRC.

p. Commander, U.S. Army Materiel Command (AMC). The Commander, AMC will:

(1) support the DCS, G-4 in completing the rationalization of the Logistics Domain IT portfolio no later than 120 days from the date of this directive.

(2) ensure the update of the resultant target environment and SV-8 and annotation of decisions in the FY 17 funds certification request.

(3) migrate, in coordination with the PEO EIS and within existing resources, the Logistics Modernization Program ERP and Logistics Information Warehouse to the approved DISA DECC ERP enclave environment no later than 30 September 2018.

q. Director of Business Transformation. The Director will:

(1) lead BMA efforts to rationalize the Army BMA portfolio no later than 180 days from the date of this directive.

(2) coordinate and lead system analysis for potential inclusion of non-ERP systems in the DISA DECC ERP hosting environment to maximize the potential of an engineered solution to BMA system hosting.

(3) review BMA system and application migration efforts quarterly within the Army Business Council starting no later than 90 days from the date of this directive.

(4) assist Army commands, HQDA staff principals, and the CIO/G-6 with system analysis for migration efforts.

(5) facilitate Army commands' access to training on best practices for application rationalization methodologies.

r. Army Deputy Chief Management Officer. The Deputy Chief Management Office will cochair the Special Data Center and migration-focused MIRC with the Deputy CIO/G-6.

s. Commander, Second Army. In coordination with ARCYBER, the commander will:

(1) no later than 90 days from the date of this directive and in coordination with AAMBO, provide the CIO/G-6 with a POA&M to facilitate the migration of all public-facing Web sites to an approved demilitarized zone extension or enterprise-hosting environment. Additional details are in reference s.

(2) no later than 90 days from the date of this directive, provide the requirements for the computer network defense service provider (CNDSP), commensurate with effect levels, to AAMBO for inclusion in standard contracting language that supports application migration security requirements. AAMBO will include these requirements in the Army commercial cloud contract vehicle, SLAs, and any other Army-approved contract vehicles.

(3) no later than 90 days from the date of this directive, develop and publish the concept of operations for management of applications migrated to enterprise environments. This concept will incorporate operation and maintenance strategies for all approved enterprise hosting options, including the commercial cloud, AEDCs, and DISA enterprise hosting options (DISA DECC, milCloud, and milCloud Plus).

(4) no later than 120 days from the date of this directive, conduct an event-driven CBA, including development of COAs, to determine Second Army's ability to deliver IT capabilities to the HRC (Fort Knox), FORSCOM (Fort Bragg), and USARC (Fort Bragg) customer bases at or above existing service levels and at or below existing costs. Pending the successful outcome of the CBA for Second Army assuming ownership of the AEDCs at HRC (Fort Knox), FORSCOM (Fort Bragg), and USARC (Fort Bragg):

(a) develop a POA&M for standardizing the infrastructure, operation, and maintenance of identified AEDCs.

(b) develop and implement AEDC application onboarding processes, including standardization of SLAs.

(c) develop and implement a standardized methodology for onboarding applications into AEDCs, prioritizing applications for onboarding and distributing them among the AEDCs.

(5) no later than 180 days from the date of this directive and in coordination with AAMBO, outline required CNDSP roles and responsibilities incumbent upon enterprise hosting environments, including commercial CSPs, from which Army commands operate for ARCYBER to execute its CNDSP role for the Army, including navigating within the commercial CPS environment when required.

(6) no later than 180 days from the date of this directive, develop a POA&M and cost estimate for consolidating multiple data processing facilities and data centers at Army posts, camps, and stations in accordance with DoD FY 18 requirements for data center consolidation. Use the cost estimate to inform POM 19–23.

(7) no later than 180 days from the date of this directive and in coordination with AAMBO, develop and publish common services standards for commercial service provider hosting solutions based on current Army policy governing commercial hosting.

(8) pending the successful outcome of the CBA for Second Army assuming ownership of the AEDCs at HRC (Fort Knox), FORSCOM (Fort Bragg), and USARC (Fort Bragg), accept the transition of any AEDC Second Army does not currently own or operate and facilitate the standardization of infrastructure, service provisioning, costing, and operations and maintenance.

(9) plan, prepare, and execute, within existing resources, the Army Private Cloud Pilot at Redstone Arsenal to provide recommendations on the utility and cost-effectiveness of an on-premises Army Private Cloud as a viable migration planning and enterprise hosting option.

t. Forces Command. No later than 120 days from the date of this directive, in concert with Second Army, the Commander, FORSCOM will conduct an event-driven CBA, including the development of COAs, to determine Second Army's ability to deliver IT capabilities to FORSCOM's customer-base at or above existing service levels and at or below existing costs.

u. Reserve Command. No later than 120 days from the date of this directive, in concert with Second Army, the Commander, USARC will conduct an event-driven CBA, including the development of COAs, to determine Second Army's ability to deliver IT capabilities to USARC's customer-base at or above existing service levels and at or below existing costs.

9. Coordinating Instructions

a. This plan is effective upon receipt for planning. Execution occurs in accordance with the timelines in the following table. All references are available at the Army

CIO/G-6 portal, which requires a common access card: https://army.deps.mil/army/cmds/hqda_ciog6_Project/ADCCP/CloudDocRepository/default.aspx.

Date	Action	Office of Primary Responsibility
NLT 5th working day of each month	Report application migration status to AAMBO to ensure the Army has a centralized, accurate database for application migrations.	Organizations not using AAMBO
NLT 90 days after directive signed	Begin MIRC.	CIO/G-6, Deputy Chief Management Officer
NLT 90 days after directive signed	Complete an application rationalization analysis and disposition decision of all systems and applications within the command's portfolio, including certification by general officer/member of Senior Executive Service.	Army Commands, Proponents
NLT 90 days after directive signed	Finalize migration planning for the next POM cycle.	Mission Area Leads
NLT 120 days after directive signed	Begin reporting Army application migration progress to Senor Review Group quarterly.	AENC Chair
NLT 120 days after directive signed	Complete an application rationalization and disposition decision for all systems and applications within the domain.	All Domain Leads
NLT 120 days after directive signed	Complete an event-driven CBA, including development of COAs, to determine Second Army's ability to deliver IT capabilities to the HRC (Fort Knox) and FORSCOM and USARC (Fort Bragg) customer bases at or above existing service levels and at or below existing costs.	Second Army
NLT 120 days after directive signed	Complete, in concert with Second Army, an event-driven CBA, including the development of COAs, to determine Second Army's ability to deliver IT capabilities to the FORSCOM and USARC customer bases, respectively, at or above existing service levels and at or below existing costs.	DCS, G-1 (HRC), FORSCOM, USARC
NLT 180 days after directive signed	Complete an application rationalization, analysis, and disposition decision for all systems and application within the BMA portfolio and record the results. Results inform the submission of the FY 17 organizational execution plan and FY 17 BMA portfolio reviews. Provide Army CIO/G-6 (Personnel and Readiness) with the mission area-endorsed application migration list.	Office of Business Transformation, BMA

Date	Action	Office of Primary Responsibility
NLT 180 days after directive signed	Complete an application rationalization, analysis, and disposition decision for all the systems and applications within the Enterprise Information Environment, Intelligence, and Warfighting Mission Areas. Provide Army CIO/G-6 Personnel and Readiness with the mission area-endorsed application migration list.	CIO/G-6; DCS, G-2; DCS, G-3/5/7; Mission Area Leads
NLT 180 days after directive signed	Complete BMA FY 16 portfolio reviews and lock BMA target environment. Update Enterprise Knowledge Repository.	BMA Domains
NLT 180 days after directive signed	Complete migration analysis of BMA portfolio with specific emphasis on non-ERP systems capable of being hosted within the ERP DISA DECC hosting environment.	Office of Business Transformation, BMA Domains
NLT 180 days after directive signed	Complete ERP migration to DISA DECC ERP hosting environment.	ERP System Owners
NLT 60 days after IPPS-A Increment 2 fielding	Coordinate with PEO EIS to remove IPPS-A Increment 1 from AEDC at HRC (Fort Knox).	DCS, G-1 (HRC)
NLT 31 January 2017	All Army commands complete transition to Microsoft Windows 10 NLT 31 January 2017. Organizations unable to meet the suspense may request a waiver through the appropriate process the Army CIO/G-6 and DoD established.	All Army commands
NLT 31 June 2017	Complete integration of ADCCP tracking tool into APMS.	CIO/G-6
Pending successful outcome of an event-driven CBA at HRC (Fort Knox)	Transition the DCS, G-1 (HRC) Fort Knox Data Center (FKNX_KY_HG1_01) to Second Army in coordination with ARCYBER.	DCS, G-1 (HRC)
Pending successful outcome of an event-driven CBA at FORSCOM (Fort Bragg)	Transition the FORSCOM Fort Bragg Data Center (FBRG_NC_FOR_01) to Second Army in coordination with ARCYBER.	FORSCOM
Pending successful outcome of an event-driven CBA at USARC (Fort Bragg)	Transition the USARC Fort Bragg Data Center (FBRG_NC_ARC_01) to Second Army in coordination with ARCYBER.	USARC
Pending successful outcome of an event-driven CBA at HRC (Fort Knox), FORSCOM (Fort Bragg), and USARC (Fort Bragg)	Accept the transition of the DCS, G-1 (HRC) Fort Knox Data Center (FKNX_KY_HG1_01), and Fort Bragg FORSCOM (FBRG_NC_FOR_01) and USARC (FBRG_NC_ARC 01) Data Centers to Second Army in coordination with ARCYBER.	Second Army in coordination with ARCYBER

b. The MIRC governance forum is the office of primary responsibility for monitoring the status of the implementation tasks and ensuring compliance with the directive.

c. No later than 90 days from the date of the directive, all Army commands must complete their application rationalization. No later than 120 days from the date of the directive, all domains must complete their application rationalization. No later than 180 days from the date of the directive, all mission areas must complete their rationalization.

d. No later than the end of the fourth quarter FY 18, Army commands will virtualize and Web-enable all enterprise systems and complete migration to an approved enterprise hosting environment, contingent upon the availability of enterprise hosting environments. All non-enterprise systems (systems that provide services and data to users within host installation boundaries) operating from local IPN hosting facilities consolidate to the approved IPN on the post, camp, or station from which it is operating, in accordance with the defined IPN list in enclosure 4. Army commands approved to operate SPPNs will continue to operate the SPPNs at approved locations. For ERP systems, the priority for migration remains DISA DECC ERP enclaves. For enterprise systems and applications, the priority for migration remains the commercial cloud and AEDCs. Only those systems and applications approved for participation in the APC-E (pilot) at Redstone Arsenal are authorized to us the APC-E as their enterprise hosting option at this time.

e. Army commands contracting for commercial cloud services are only authorized to use CSPs that host data in clouds that are within the United States or its outlying areas, as defined in the Federal Acquisition Regulation 2.101 (reference w), or in OCONUS locations that are within U.S. control and not subject to host-nation or regional laws through treaty or other circumstance.

f. No later than 31 December 2017, Army commands will, within existing resources, migrate all enterprise systems with low security impact levels (data impact levels 1 and 2) in reference h and public-facing Web sites to an approved demilitarized zone extension or enterprise hosting environment.

g. No later than 30 September 2018, Army commands will, within existing resources, migrate enterprise systems with higher security impact levels (data impact levels 4 and 5) to approved enterprise hosting options, including DISA DECCs, MilCloud/MilCloud Plus, or an AEDC. Use of on- or off-premises commercial cloud service offerings is an alternative if they meet the data and security requirements in reference h and the migration requirements in reference d.

h. Army commands will adhere to the process flow outlined in the Application Migration Process Overview (enclosure 3). This overview illustrates a high-level overview (figure 1) and a detailed view (figure 2) of the application migration process.

i. Closure and consolidation efforts for Army data centers support the migration of applications to enterprise hosting environments. Army commands must submit a data center closure report to the Army CIO/G-6 no later than 30 days after closing a data center. For data centers already closed for more than 30 days, the owning Army organization must submit a data center closure report no later than 30 days from the date of this directive.

j. Army commands will use the MIRC governance process to formally submit requests to defer closure or redesignate a data center (for example, from IPN to SPPN) to the AENC for review and approval.

k. Army commands will continue to report their system and application rationalization and migration status at the quarterly Chief Information Officer Executive Board meeting. The reporting instructions the Executive Board issues before the meeting will prescribe the format for the reports.

l. Army commands are authorized to bundle applications as part of the CBA process. If doing so, the organization will determine the best methodology for bundling applications within its portfolio.

m. Organizations may opt not to use AAMBO, contingent upon their ability to meet AAMBO standards the ASA (ALT) established and with the Army CIO/G-6's approval. Regardless, all organizations must report application migration status to AAMBO by the 5th working day of each month to ensure that the Army has a centralized, accurate database for application migrations

n. Based on the data center closures identified in enclosure 4, table 2 of the implementation plan, the MIRC will assess operational effects on Army organizations, including the consideration of CBAs for alternate application hosting locations.

o. All Army commands transitioning to and/or using an approved enterprise hosting environment will remain compliant with the Department of the Army Records Information Management System for retention and records management in accordance with reference q.

p. Army commands must remain compliant with all Army and DoD data-sharing and data-management requirements. All Army commands transitioning to any approved enterprise hosting environment must ensure the IT services and data identified for transition are compliant with DoD Instruction 8320.02 (reference o), and AR 25-1 (reference p) before completing the transition.

(1) Data, information, and IT services are considered enablers of information sharing within DoD. Data, information, and IT services will be made visible, accessible, understandable, trusted, and interoperable throughout their life cycles for all authorized users. Authorized users include DoD consumers and mission partners, subject to law, policy, data rights, and security classifications.

(2) Data sources transitioning to enterprise hosting environments where data is created by the organization and shared across the enterprise (including IT services and data transitioning to the commercial cloud) require registration and approval as an Authoritative Data Source (ADS) in the 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 is a key enabler for making data visible, accessible, and understandable because it is an enterprise service that streamlines the search for and access to data, and provides a set of tools to register and discover data services across DoD.

(3) An ADS is a recognized or official data production source with a designated mission statement or source/product to publish reliable and accurate data for customers to subsequently use. An ADS may be the functional combination of multiple, separate data sources and consists of three items: data need, system, and data producer. Authoritative data elements are data elements the system and data producer own, create, control, and store.

(4) All IT capabilities and content hosted in an approved enterprise hosting environment must adhere to standards in the DoD IT standards registry or to the standards specified in the applicable Army COE standard view.

q. Army commands may submit an application waiver request, along with appropriate justification, if they are not able to meet the requirements to migrate their application to an approved enterprise hosting environment in the required time. The waiver types permitted are: disposition waiver, existing contract waiver, and the Information Technology Approval System (ITAS) waiver. Waiver request packages will include a memorandum with justification for the waiver, POA&M, and timeline for completion (disposition waivers) (not to exceed 30 September 2020). Army commands must submit their waiver request packages to the MIRC for review and approval, routed from the requesting organization through command channels to the senior general officer/member of the Senior Executive Service for endorsement and submission to the MIRC.

(1) Disposition Waiver. The disposition waiver includes the terminate, modernize, and sustain dispositions and is available for Army system and application owners who will not complete their disposition by 30 September 2018.

(2) Existing Contract Waiver. Army system and application owners who are already operating in an approved enterprise hosting facility (including commercial CSPs) and who have or will sign a contract or SLA within 45 days from the date of this directive may maintain the existing contract or SLA under the following conditions:

(a) Contact AAMBO and provide system and application information. System and application owners will also provide the MIRC and appropriate mission area governance forum with a copy of the contract or SLA within 45 days from the date of

this directive. By reviewing the contract, the MIRC and mission area governance forum will be able to review and assess the current level of risk to be accepted and determine whether it complies with the Army migration guidelines outlined in this directive.

(b) Before executing follow-on option years or renewing the SLA or contract, system and application owners will contact AAMBO, complete an application review and CBA, and provide the CBA to the appropriate domain and mission area governance forums. The forums will review and consider the waiver for endorsement and forward to the MIRC for approval.

r. Army commands are responsible for all costs associated with funding their system or application migration, including developing, modernizing, migrating, and hosting systems or applications. Organizations will execute their plans, within existing resources, according to the milestones in this directive. If required, organizations will seek relief during the annual midyear review and prioritization process.

(1) ITAS (formerly Goal 1) waiver requirements remain in effect for the expenditure or commitment of funds related to data center IT investments, including hosting services, hardware, software, storage, or other services associated with a data center before executing funds, regardless of whether the item is purchased through Computer Hardware, Enterprise Software and Solutions (CHESS). All new applications and systems, even if developed in an enterprise hosting environment, require an approved CBA or waiver. Approved ITAS waivers are valid for 1 year and are reassessed annually. The ITAS memorandum (reference k) provides additional details.

(2) Because many of the actions necessary to implement this directive require the reprioritization of existing and programmed funds during FYs 16–18, some requirements may not be achieved by 30 September 2018. Army commands and Program Executive Groups are responsible for planning and programming the residual costs associated with migrating remaining systems and applications and finalizing the transition to Windows 10, and for all costs associated with hosting systems or applications during POM 19–23.

(3) To leverage resource availability to implement the actions directed in this directive, Army commands, portfolio managers, and system and application owners must consider the following resourcing strategy (as applicable):

(a) Reprioritize existing hardware refresh or major software upgrade resources to cover costs during the year of execution and budget year.

(b) Increase resource flexibility by performing rationalization with an emphasis on terminating duplicative systems and applications.

(c) Reprioritize within existing resources to address resource gaps before engaging the Army Budget Office or DCS, G-8 for additional resource support.

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

(e) Provide key AAMBO artifacts, including but not limited to, the Migration Assessment Report with application hosting cost and work breakdown structure, to the organization resource manager, management decision execution package manager, Program Executive Group, and Program Budget Assessment Team for resource validation.

(2) Suborganizations or application owners must coordinate contracts within the organization before engaging external agencies. Specifically, if an entity is contracting for commercial cloud services, an organizationwide approach is encouraged to ensure that existing contracts are checked and coordinated to minimize duplication of contracting efforts and use all assets available to the Army organization.

s. As directed, Army commands will provide representation to the MIRC.

t. Army commands, in concert with the MIRC, will assess the feasibility, suitability, and acceptability of closing SPPNs identified in enclosure 4, table 2, including identifying SPPNs requiring exemption from closure.

u. Army commands will use systems and application modernization checklists and guides provided by AAMBO.

v. Army commands will support Second Army with the development of the concept of operations for managing applications migrated to enterprise hosting environments.

10. The Under Secretary of the Army and Vice Chief of Staff, Army are authorized to approve revisions and changes to this plan.

11. The implementation plan point of contact is Mr. Attila (A.J.) Bognar, Army Data Center Consolidation Program Division Chief, Office of the Army CIO/G-6, 703-697-7615 or attila.j.bognar.civ@mail.mil.

APPLICATION MIGRATION PROCESS FLOW

The Army's overarching process flow for migrating applications includes a high-level overview and detailed application migration process flow. The high-level overview (figure 1) is intended to portray a quick snapshot of the process without the specific details. The detailed process flow (figures 2 through 7) provides specific guidance for each step of the process. All figures are subject to revision as the processes are further refined and continue to mature.

High-Level Overview of End-to-End Application Migration

The high-level overview follows a basic six-step process to migrate Army enterprise systems to an approved enterprise hosting facility: (1) discovery and portfolio analysis, (2) migration readiness assessment, (3) cost-benefit analysis, (4) migration planning, (5) execute migration, and (6) quality assurance and steady state.

Figure 1 represents the consolidated view of the entire six-step process for application migration. It is intended to be a visual outline of the application migration process, with the detailed description in each of the subsequent steps. System and application owners should refer to the appropriate step within figures 2 through 7 for specific actions tied to each step of the application migration process.

End-to-End Application Migration Overview

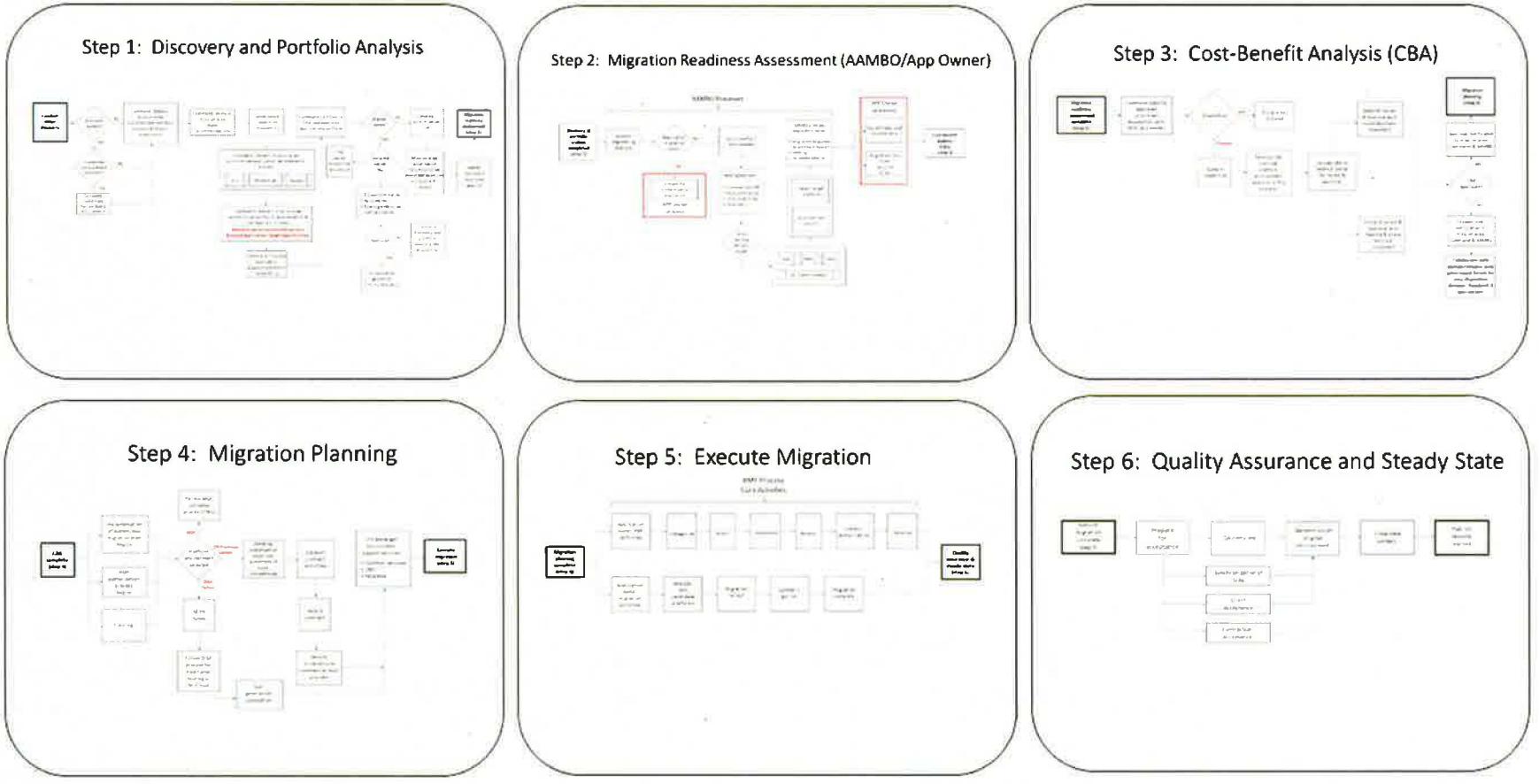

Figure 1. High-Level Overview: End-to-End Process Flow

End-to-End Application Migration Detailed Process Flow

Step 1: Discovery and Portfolio Analysis

Figure 2, step 1 includes completing system and application discovery; binning; rationalization; and disposition (kill, sustain, or modernize). Army commands are ultimately responsible for ensuring that they document all systems and applications within their information technology (IT) portfolio in the Army Portfolio Management System (APMS), and properly bin and rationalize them (as outlined in reference i). As part of the governance process, Army commands must collaborate with the domain and mission area to eliminate duplicate, inefficient, costly, or low-performing applications in favor of enterprise, Web-enabled, virtualized applications that are capable of providing services across the Army organization, domain, and mission area.

Portfolio synchronization among the Army organization, domain, and mission area is iterative and critical for the organizations to produce an endorsed application portfolio that meets the agreed-to disposition. After the application portfolio is finalized, the Army organization will determine whether it needs a waiver for any of its applications and will submit a waiver if necessary. (The waiver process is explained in detail in enclosure 2). If the Army organization does not require a waiver, it will develop the migration prioritization list. Mission area governance forums will provide the endorsed application list to the Army Chief Information Officer (CIO)/G-6 for review and approval. After approval, the Army CIO/G-6 provides the Army Application Migration Business Office (AAMBO) with the approved applications migration list before the Army organization may begin its migration readiness assessment.

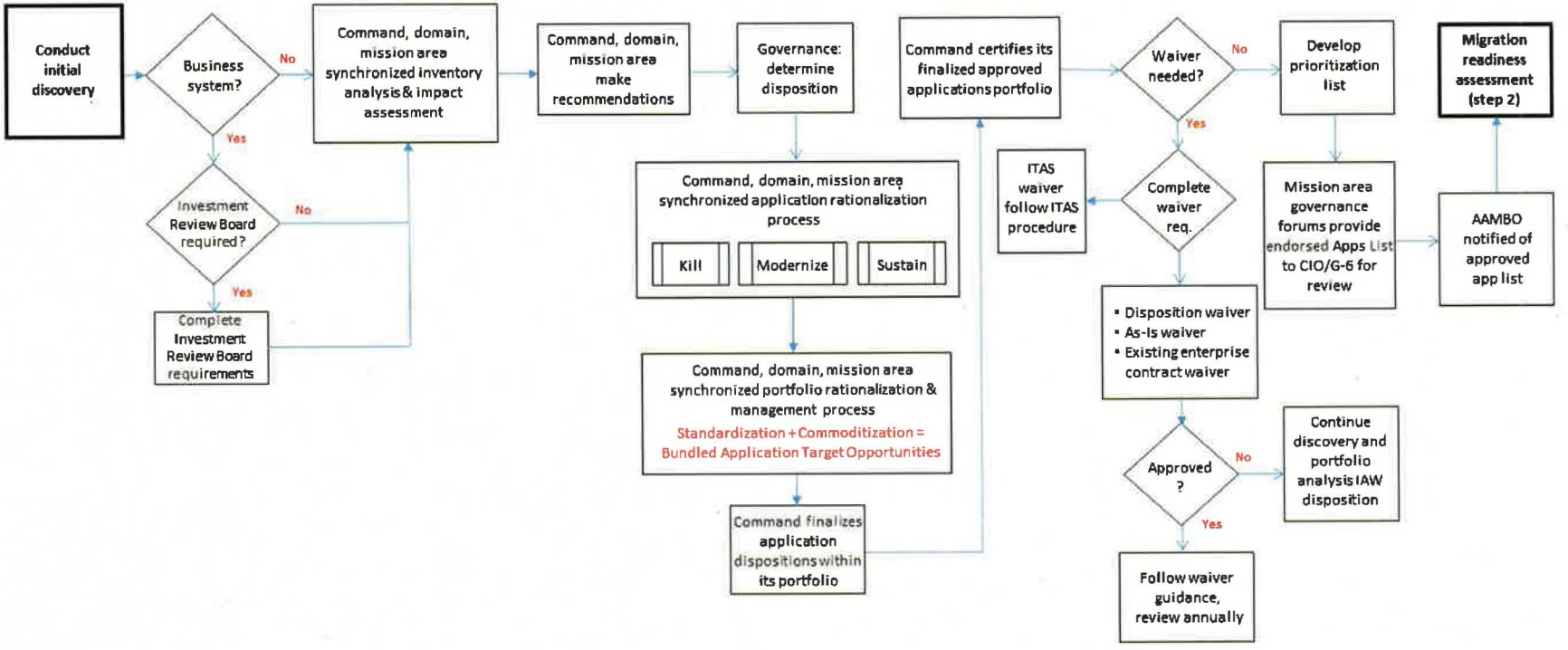

Figure 2. Step 1: Discovery and Portfolio Analysis

Step 2: Migration Readiness Assessment (AAMBO/Application Owner)

AAMBO

AAMBO continues to serve as the Army's single point of contact for assisting Army commands in planning their system and application migrations. Although Army commands may contact and collaborate with AAMBO anywhere within the application migration process, they are required to contact AAMBO and provide their system information at this step within the process. Activities include:

- providing assistance in recommending the most cost-effective and technically feasible hosting and support strategies,
- providing the commercial cloud contract vehicle for the Army application migration (and Army-approved contracting language for other approved cloud contract vehicles), and
- supporting application owners throughout the migration process (figure 3).

Perform Migration Readiness Assessment

System owners must provide AAMBO with a valid Army Information Technology Registry number to verify that they have registered their system or application in APMS before AAMBO can begin the engineering analysis. After AAMBO receives the required system information for the migrating enterprise system, AAMBO will begin the systems engineering analysis to assess whether the application is ready to migrate. If it is not ready to migrate, then AAMBO will request that the application owner complete all modernization activities in accordance with the AAMBO-provided modernization checklist to continue the modernization evaluation. If the system or application is ready to migrate, AAMBO will recommend a target enterprise hosting environment.

The actions outlined in this step facilitate an informed recommendation of the service delivery model and hosting options. After AAMBO provides the application owner with the cost estimate and migration readiness assessment report, the application owner performs the total cost of ownership and migration cost activities which are necessary actions to build the cost-benefit analysis (CBA).

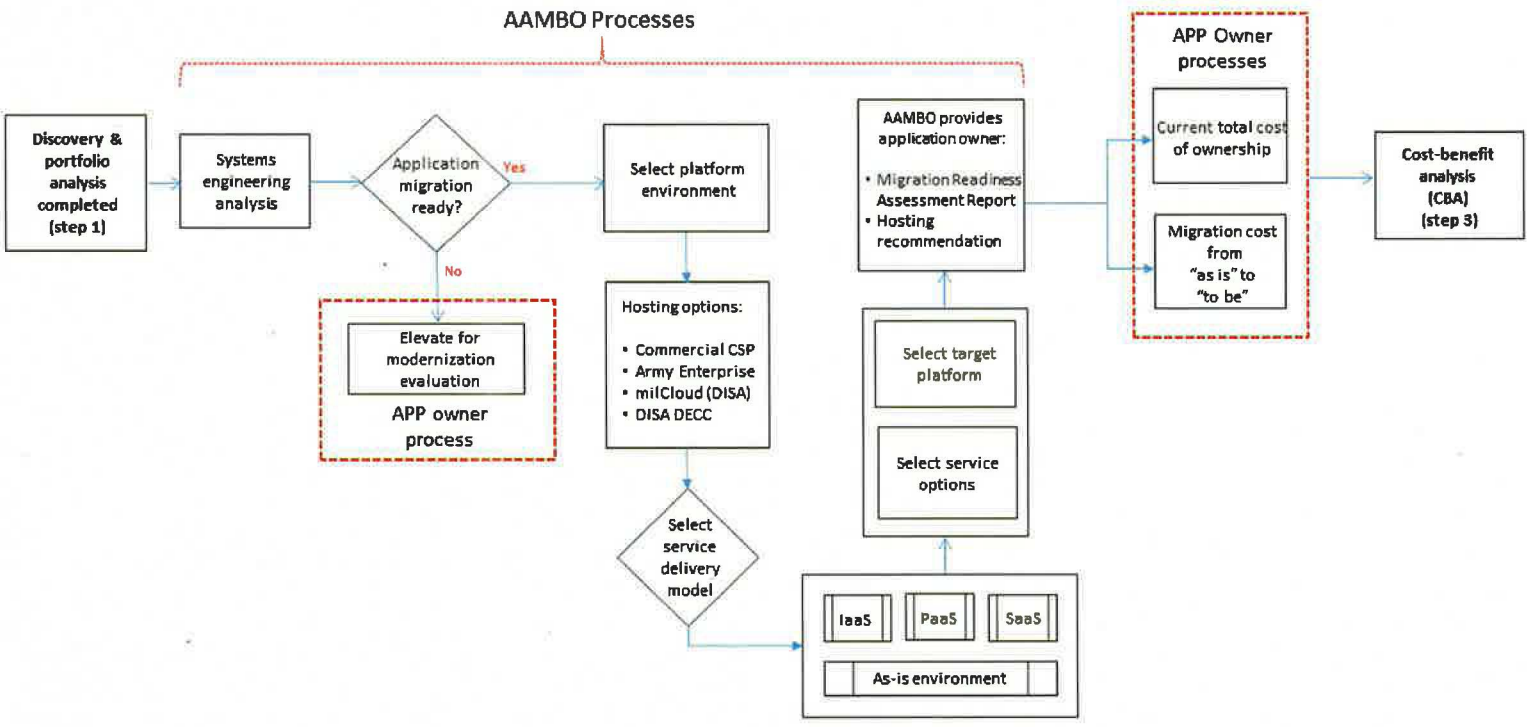

Figure 3. Step 2: Migration Readiness Assessment

Step 3: Cost-Benefit Analysis

For new systems and applications, and those with a disposition of sustain or modernize, the Army organization must complete an Army IT CBA and forward it through the appropriate domain and mission area governance forums for review and endorsement (figure 4). Ultimately, the CIO/G-6 reviews and either approves or rejects the CBA in parallel with the Deputy Assistant Secretary of the Army (Cost and Economics) (DASA-CE), who validates the cost methodology and structure (reference f).

Army commands are responsible for all costs associated with developing, migrating, and hosting their systems and applications. The coordinating instructions list additional funding guidance. All Army commands purchasing hosting services, hardware, software, storage, or other services associated with a data center must have an approved Information Technology Approval System (ITAS) waiver before executing funds, regardless of whether the item is purchased through Computer Hardware, Enterprise Software, and Solutions (CHESS), in accordance with the CIO/G-6 ITAS waiver policy (reference k).

Step 4: Migration Planning

The migration planning step includes all actions necessary to prepare the enterprise system to transition to the approved enterprise hosting environment (figure 5). After CBA approval, the CIO/G-6 notifies the Migration Implementation and Review Council, the Army organization, and AAMBO, and the Army organization initiates the following activities simultaneously: migration plan implementation, the Risk Management Framework (RMF) authorization process, and necessary training. Depending on the enterprise hosting environment selected, associated activities include development of the statement of objective/statement of work, contracting activities, coordination of the service level agreement (SLA), service initiation for the commercial cloud service provider hosting option, and transferring funds/military interdepartmental purchase request.

If the Army organization selects the Defense Information Systems Agency (DISA) enterprise hosting option, it will coordinate with DISA for connectivity to the cloud access point. The on-premises connection process will be further developed in accordance with the Army Private Cloud–Enterprise (APC-E) (pilot) Implementation Plan; for now, it is designated as "to be determined." After completing these activities, the organization will initiate target environment support services, including integration of common services (whether provided by DISA or Second Army, in coordination with U.S. Army Cyber Command (ARCYBER)), computer network defense, and help desk support.

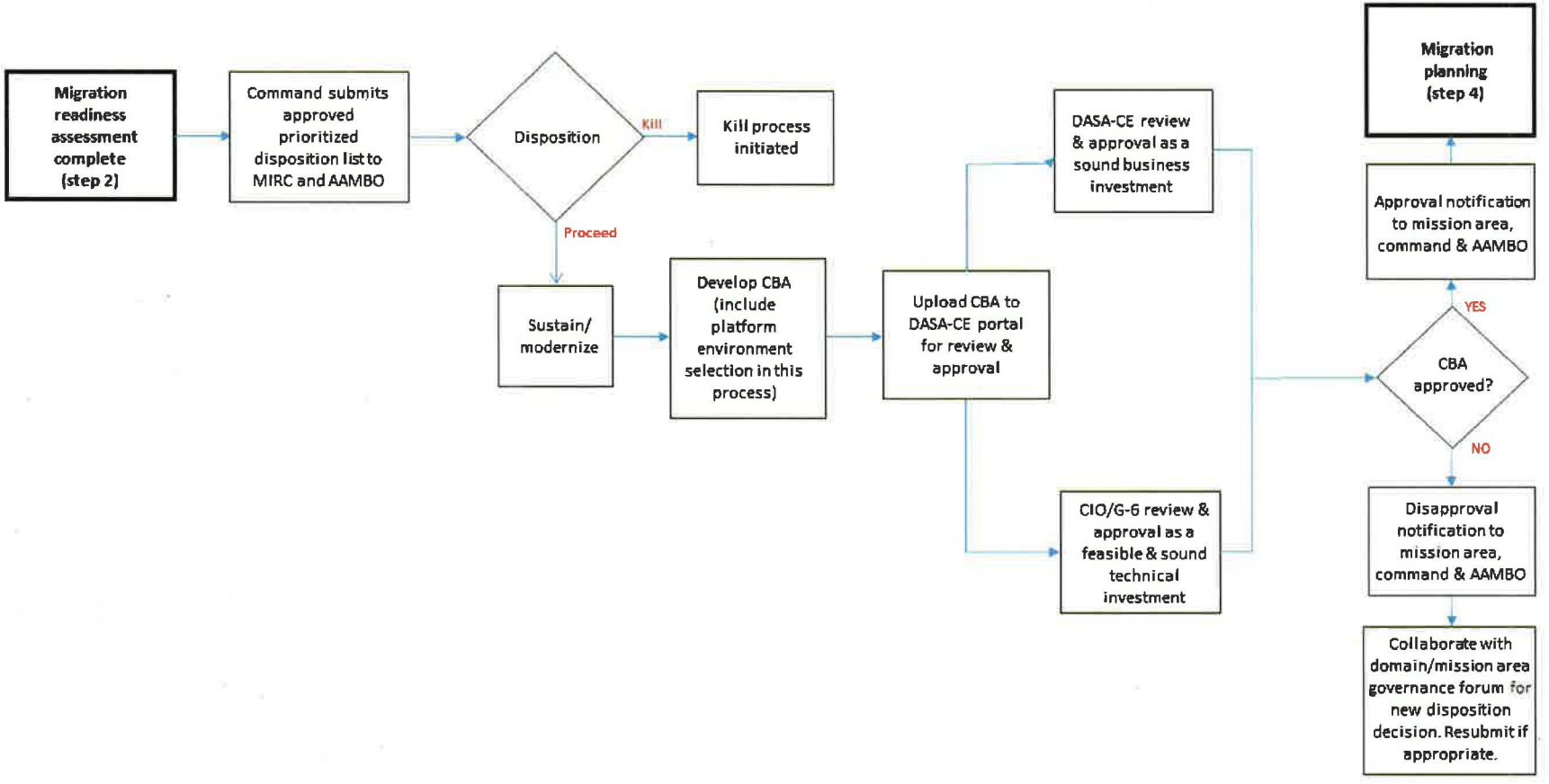

Figure 4. Step 3: Cost-Benefit Analysis

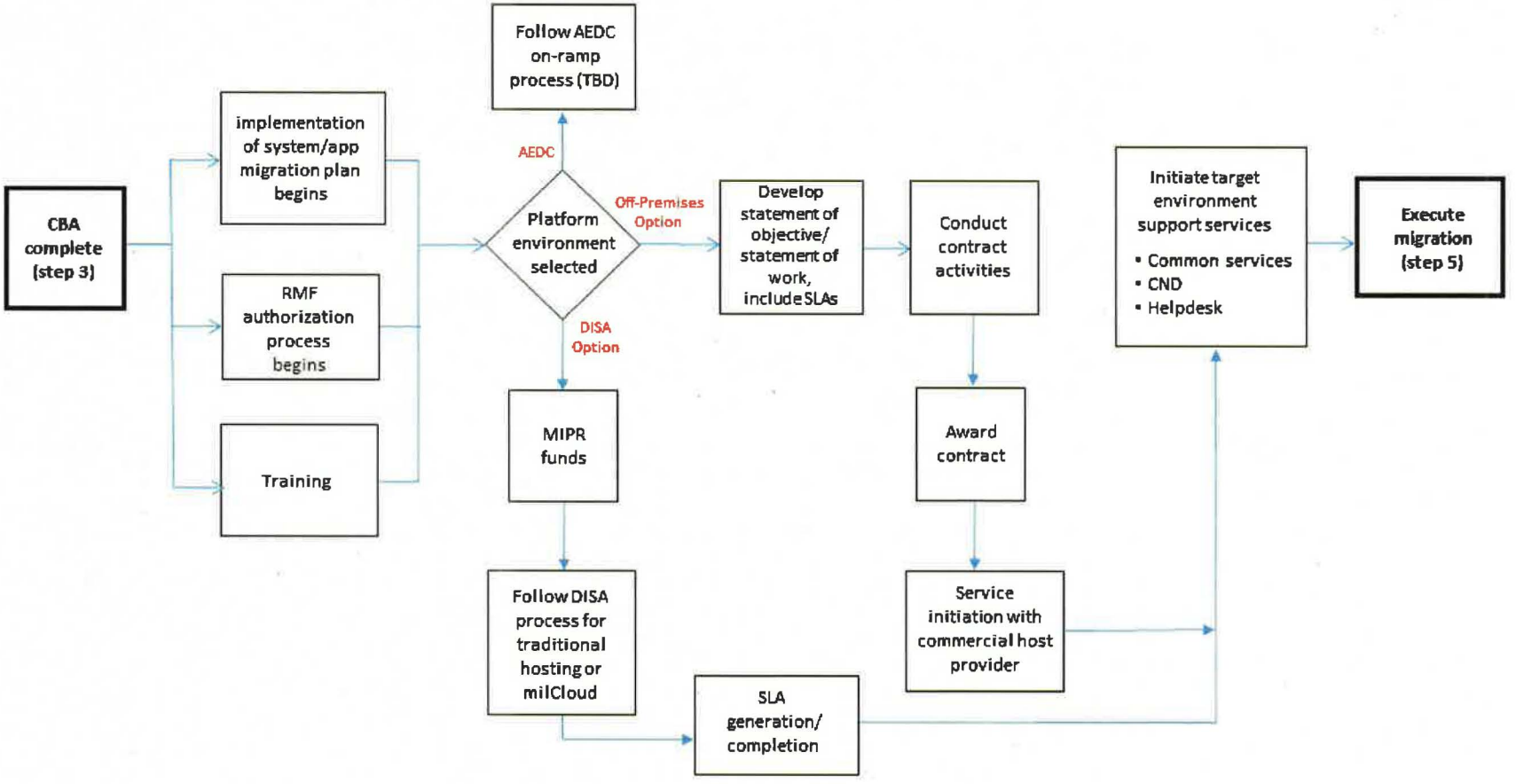

Figure 5. Step 4: Migration Planning

Step 5: Execute Migration

After completion of migration planning, a simultaneous two-pronged process begins to ensure that migration activities align for a successful cutover (figure 6). The application owner begins the RMF process to obtain an Interim Authorization to Test and subsequently an Authority to Operate. The application owner analyzes and tests the capability in its new environment, then migration rollout activities begin, followed by the cutover. After completion of the RMF process and application owner activities, the migration is complete and the transition into quality assurance and steady state begins.

Step 6: Quality Assurance and Steady State

After completion of migration activities, the system or application owner will complete "go live" activities, which include the synchronization of SLAs, client acceptance, and contractual acceptance (figure 7). In tandem, the quality assurance process begins. After acceptance of the new environment, the original environment will be decommissioned (in accordance with reference g) and data center closed. AAMBO will collect and publish lessons learned for other stakeholders to use.

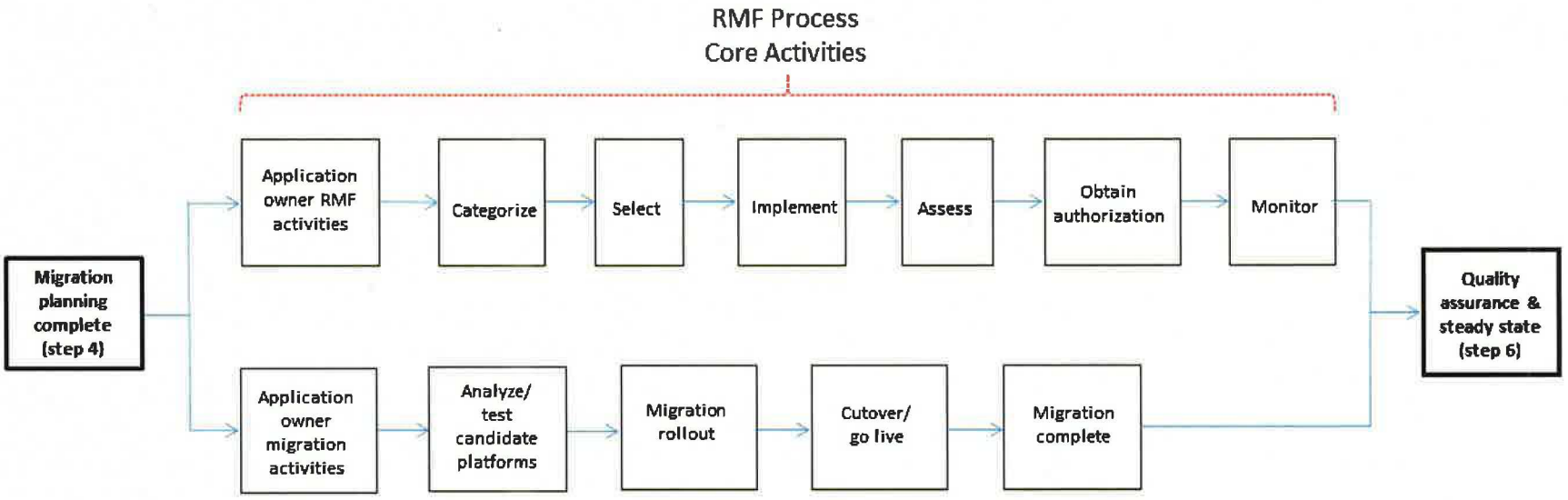

Figure 6. Step 5: Execute Migration

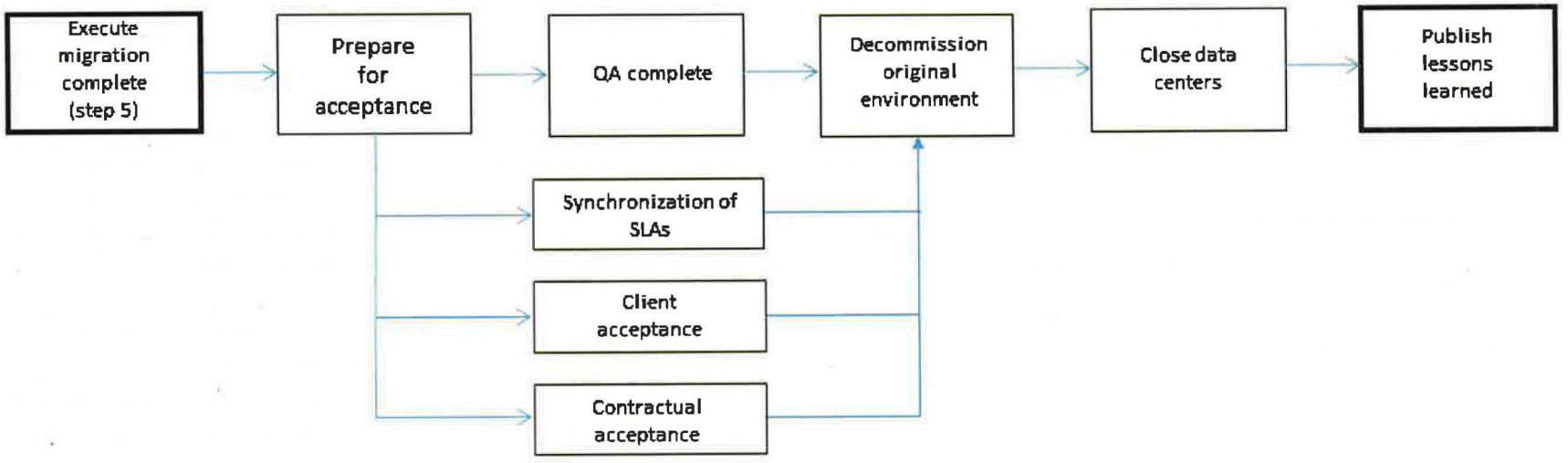

Figure 7. Step 6: Quality Assurance and Steady State

TABLE 1: AUTHORIZED ALLOCATIONS OF COMPUTING CENTERS BY INSTALLATION DURING FY 25

Army Installations	IPN	SPPN	ISN*	GSU**	AEDC	APC-E***	DISA DECC
Alabama							
JTF-HQ ARNG	1						
Fort Rucker		1	1				
Redstone Arsenal		10				1	
Alaska							
JTF-HQ ARNG	1						
Fort Greely			1				
Fort Wainwright			1				
Joint Base Elmendorf-Richardson		1	1				
Arizona							
JTF-HQ ARNG	1						
Camp Navajo (ARNG)			1				
Fort Huachuca		1	1				
Yuma Proving Ground		1	1				
Phoenix (AZ/NV Area Office)		1					
Arkansas							
JTF-HQ ARNG	1						
Camp Joseph T. Robinson (ARNG)			1				
Fort Chaffee Maneuver Training Center (ARNG)			1				
Pine Bluff Arsenal		1	1				
Wynne Area Office		1					
Royal-Blakely Mountain Power Plant		1					
California							
JTF-HQ ARNG	1						
Camp Beale			1				
Camp Cooke			1				
Camp Haan			1				
Camp Roberts (ARNG)			1				
Camp San Luis Obispo (ARNG)			1				
Fort Hunter Liggett		2	1				
Fort Irwin		2	1				
Los Alamitos Joint Forces Training Base			1				
Military Ocean Terminal Concord			1				

Army Installations	IPN	SPPN	ISN*	GSU**	AEDC	APC-E***	DISA DECC
Naval Base Point Loma			1				
Parks Reserve Forces Training Area			1				
Presidio of Monterey		3	1				
San Joaquin Depot							
Sharpe Facility							
Stockton's Rough & Ready Island							
Tracy Facility							
Sierra Army Depot		1	1				
Sacramento Resident Office		1					
Monterey Project Office		1					
Folsom Resident Office		1					
Folsom JFP Office		1					
Eureka Field Office		1					
Black Butte Field Site		1					
Eastman Lake Field Site		1					
Englebright Lake Field Site		1					
Hensley Lake Field Site		1					
Kaweah Laker		1					
New Hogan Lake Field Site		1					
Pine Flat Field Site		1					
Oakland - Stanislaus Field Site		1					
Porterville - Success Field Site		1					
Lake Isabella Field Site		1					
Lake Isabella Field Site 2		1					
West Sacramento - Valley Resident Office		1					
Lake Mendocino Field Site		1					
Lake Sonoma Field Site		1					
Sausalito Field Site		1					
Colorado							
JTF-HQ ARNG	1						
Fort Carson		6				1	
Fort Logan National Cemetery			1				
Pueblo Chemical Depot		1	1				
Colorado Springs Field Office		1					
Grand Junction Field Office		1					
Connecticut							
JTF-HQ ARNG	1						

Army Installations	IPN	SPPN	ISN*	GSU**	AEDC	APC-E***	DISA DECC
Camp Niantic (ARNG)			1				
District of Columbia							
JTF-HQ-ARNG	1						
DC Armory XXXX		1					
Delaware							
JTF-HQ ARNG	1						
Bethany Beach Training Site (ARNG)							
District of Columbia							
Fort Lesley J. McNair			1				
Florida							
JTF-HQ ARNG	1						
Miami	1						
Homestead Air Reserve Base	1						
Camp Blanding (ARNG)			1				
Georgia							
JTF-HQ ARNG	1						
Camp Frank D. Merrill			1				
Fort Benning		8	1				
Fort Gillem		1					
Fort Gordon		7	1				
Fort Stewart		2	1				
Hunter Army Airfield			1				
Robins Air Force Base		1					
63rd Regional Support Command (USACE)		1					
Morrow Regulatory Field Office		1					
Russell Lake Project Site		1					
Hartwell Lake Project Site		1					
Guam							
JTF-HQ-ARNG	1						
Fort Guam XXXXX		1					
Hawaii							
JTF-HQ ARNG	1						
Fort DeRussy (MWR Resort)		1					
Hale Koa Hotel		1					
Fort Shafter					1		
Kunia Field Station			1				

Army Installations	IPN	SPPN	ISN*	GSU**	AEDC	APC-E***	DISA DECC
Pohakuloa Training Area			1				
Schofield Barracks		1	1				
Tripler Army Medical Center			1				
Wheeler Army Airfield			1				
Idaho							
JTF-HQ ARNG	1						
MTA Gowen Field Boise (ARNG)			1				
Orchard Range TS Boise (ARNG)			1				
TS Edgemeade Mountain Home (ARNG)			1				
Illinois							
JTF-HQ ARNG	1						
Charles M. Price Support Center			1				
Rock Island Arsenal			1				
Champaign Engineering Research Lab		1					
Indiana							
JTF-HQ ARNG	1						
Camp Atterbury			1				
Fort Benjamin Harrison			1				
Iowa							
JTF-HQ ARNG	1						
Camp Dodge			1				
Iowa Army Ammunition Plant			1				
Kansas							
JTF-HQ ARNG	1						
Fort Leavenworth		2	1				
15th Brigade - Detention Barracks	1						
Munson Army Health Center			1				
Fort Riley		2	1				
Great Plains Joint Training Area (ARNG)			1				
Kansas Regional Training Institute (ARNG)			1				
Nickel Hall Barracks (ARNG)			1				
Smokey Hill Weapons Range (ANG)			1				
Canton Field Site		1					
Council Grove Field Site		1					
Burlington		1					

Army Installations	IPN	SPPN	ISN*	GSU**	AEDC	APC-E***	DISA DECC
Kentucky							
JTF HQ ARNG	1						
Blue Grass Army Depot			1				
Fort Campbell		7	1				
Fort Knox		2				1	
Louisville - McAlpine Locks and Dam		1					
Louisiana							
JTF HQ ARNG	1						
Camp Beauregard			1				
Fort Polk		6	1				
Peason Ridge Artillery Range			1				
Shreveport Area Office		1					
Maine							
JTF HQ ARNG	1						
MTA Deepwoods (ARNG)			1				
MTA Riley-Bog Brook (ARNG)			1				
TS Caswell (ARNG)			1				
TS Hollis Plains (ARNG)			1				
Maryland							
JTF HQ ARNG	1						
Aberdeen Proving Ground		12	1				
Adelphi Laboratory Center		2					
Camp Fretterd Military Reservation (ARNG)			1				
Fort Detrick			1				
Fort George G. Meade		7	1				
Massachusetts							
JTF HQ ARNG	1						
Camp Curtis Guild (ARNG)			1				
Camp Edwards (ARNG)			1				
Fort Devens			1				
Natick Army Soldier Systems Center		1	1				
Michigan							
JTF HQ ARNG	1						
Camp Grayling (ARNG)			1				
Detroit Arsenal		4	1				
Fort Custer (ARNG)			1				

Army Installations	IPN	SPPN	ISN*	GSU**	AEDC	APC-E***	DISA DECC
Sault Ste Marie Area Office		1					
Detroit Area Office		1					
Grand Haven Area Office		1					
Minnesota							
JTF HQ ARNG	1						
Camp Ripley (ARNG)			1				
Duluth Area Office		1					
Fort Snelling (USAR)			1				
Mississippi							
JTF HQ ARNG	1						
Camp McCain (ARNG)			1				
Camp Shelby			1				
Mississippi Ordnance Plant			1				
Arkabutla		1					
Enid Lake Field Office		1					
Grenada Lake Field Office		1					
Sardis - Mississippi Project Mgmt Office		1					
Missouri							
JTF HQ ARNG	1						
Camp Clark (ARNG)			1				
Fort Leonard Wood		7	1				
Caruthersville Test lab		1					
Branson		1					
Montana							
JTF HQ ARNG	1						
Fort Peck Dam		1					
Fort William Henry Harrison (ARNG)			1				
Nebraska							
JTF HQ ARNG	1						
Camp Ashland (ARNG)			1				
Offut Air Force Base		1					
Crofton		1					
Omaha - Missouri River Project		1					
Nevada							
JTF HQ ARNG	1						
Hawthorne Army Ammunition Depot			1				
New Jersey							

Army Installations	IPN	SPPN	ISN*	GSU**	AEDC	APC-E***	DISA DECC
JTF HQ ARNG	1						
Fort Dix, part of Joint Base McGuire-Dix-Lakehurst							
Picatinny Arsenal		4	1				
New Mexico							
JTF HQ ARNG	1						
Los Alamos Demolition Range			1				
White Sands Missile Range		1	1				
New York							
JTF HQ ARNG	1						
Fort Drum		1	1				
Watervliet Arsenal		1	1				
U.S. Military Academy		2	1				
Fort Hamilton			1				
North Carolina							
JTF HQ ARNG	1						
Camp Butner (ARNG)			1				
Camp Davis			1				
Camp Mackall			1				
Fort Bragg		5				1	
Military Ocean Terminal Sunny Point			1				
Durham		1					
Falls Lake		1					
Wilkesboro W Kerr Scott Dam and Reservoir		1					
Raleigh Field Site		1					
Asheville Field Site		1					
Washington Field Site		1					
Moncure Field Site		1					
North Dakota							
JTF HQ ARNG	1						
Camp Grafton (ARNG)			1				
Bismarck		1					
Garrison Dam		1					
Ohio							
JTF HQ ARNG	1						
Camp Perry (ARNG)			1				

Army Installations	IPN	SPPN	ISN*	GSU**	AEDC	APC-E***	DISA DECC
Camp Ravenna Joint Military Training Center (ARNG)			1				
Camp Sherman (ARNG)			1				
Wright Patterson		1					
Oklahoma							
JTF HQ ARNG	1						
Camp Gruber (ARNG)			1				
Fort Sill		3	1				
Altus Air Force Base		1					
McAlester Army Ammunition Plant			1				
Texoma Field Site		1					
Eufaula Transportation Operations		1					
Fort Gibson USACE		1					
Fort Supply Field Site		1					
Ponca City Field Site (Kaw Lake)		1					
Sand Springs Field Site (Keystone)		1					
Oologah Field Site		1					
Sallisaw Field Site (RS Kerr)		1					
Gore Field Site.(Ten Killer)		1					
Skiatook Field Site		1					
Oregon							
JTF HQ ARNG	1						
Camp Rilea (ARNG)			1				
Umatilla Chemical Depot			1				
Pennsylvania							
JTF HQ ARNG	1						
Carlisle Barracks			1				
Fort Indiantown Gap (ARNG)			1				
Harrisburg Military Post (ARNG)			1				
Letterkenny Army Depot			1				
New Cumberland Army Depot			1				
Tobyhanna Army Depot			1				
Puerto Rico							
JTF HQ ARNG	1						
Fort Buchanan			1				
Army National Guard Aviation Support Facility			1				

Army Installations	IPN	SPPN	ISN*	GSU**	AEDC	APC-E***	DISA DECC
Camp Santiago			1				
Fort Allen			1				
Roosevelt Roads Army Reserve Base			1				
Rhode Island							
JTF HQ ARNG	1						
Camp Varnum (Narragansett) (ARNG)			1				
Camp Fogarty (East Greenwich) (ARNG)			1				
South Carolina							
JTF HQ ARNG	1						
Shaw Air Force Base		1	1				
Fort Jackson		4	1				
Columbia Regulatory Office		1					
Conway Regulatory Office		1					
North Charleston Field Site		1					
Clarks Hill - Thurmond Lake Project Office		1					
South Dakota							
JTF HQ ARNG	1						
Fort Meade (ARNG)			1				
Rapid City		1					
Chamberlain		1					
Fort Randall Dam		1					
Tennessee							
JTF HQ ARNG	1						
Holston Army Ammunition Plant			1				
Kingston Demolition Range			1				
Milan Army Ammunition Plant			1				
Texas							
JTF HQ ARNG	1						
Camp Bowie			1				
Camp Bullis			1				
Camp Mabry			1				
Camp Stanley			1				
Camp Swift			1				
Camp Wolters (ARNG)			1				
Corpus Christi Army Depot			1				
Fort Bliss		5	1				
Fort Hood		4	3*				

Army Installations	IPN	SPPN	ISN*	GSU**	AEDC	APC-E***	DISA DECC
Fort Sam Houston, part of Joint Base San Antonio							
Brooke Army Medical Center							
Martindale Army Airfield			1				
Red River Army Depot			1				
Texoma Field Site		1					
Utah							
JTF HQ ARNG	1						
Camp W.G. Williams (ARNG)			1				
Dugway Proving Ground		1	1				
Hill Air Force Base		1					
Tooele Army Depot			1				
Bountiful Field Site		1					
Vermont							
JTF HQ ARNG	1						
Camp Ethan Allen Training Site (ARNG)			1				
Virginia							
JTF HQ ARNG	1						
Camp Pendleton State Military Reservation (ARNG)			1				
Fort A.P. Hill			1				
Fort Belvoir		6	1				
Fort Eustis, part of Joint Base Langley-Eustis		1	1	1			
Fort Lee			1				
Fort McNair, part of Joint Base Myer-Henderson Hall			1				
Fort Myer, part of Joint Base Myer-Henderson Hall			1				
Fort Pickett (ARNG)			1				
John H. Kerr Lake & Dam		1					
The Judge Advocate General's Legal Center and School		1	1				
Quantico Military Reservation							
National Ground Intelligence Center		1	1				
Philpott Lake		1					
Radford Army Ammunition Plant							
Rivanna Station		1					
Warrenton Training Center			1				

Army Installations	IPN	SPPN	ISN*	GSU**	AEDC	APC-E***	DISA DECC
US Virgin Islands							
JTF-HQ-ARNG	1						
Fort Virgin Islands		1					
Washington							
JTF HQ ARNG	1						
Fort Lewis, part of Joint Base Lewis-McChord		3	1*				
Yakima Training Center			1				
West Virginia							
JTF HQ ARNG	1						
Camp Dawson West Virginia Training Area (ARNG)			1				
Wisconsin							
JTF HQ ARNG	1						
Fort McCoy			1				
Camp Williams (ARNG)			1				
Kewaunee Area Office		1					
Appleton Field Office		1					
Wyoming							
JTF HQ ARNG	1						
Guernsey Maneuver Area (ARNG)			1				
Cheyenne		1					
U.S. States with no U.S. Army posts							
New Hampshire (ARNG armory posts, various individual locations statewide)							
JTF HQ ARNG	1						
Overseas							
Germany		7			2		
Korea		1			1		
Kwajalein	1	1					
Japan		1			1		
Southwest Asia		2			1		

* Multiple ISNs may exist at an installation to service high-density populations of Soldiers, civilians, and contractors.
** Geographically Separated Unit (GSU): Quantities based on number of armories in a State, or if a specific installation (Fort Eustis) is part of a joint base cluster (such as Joint Base Langley-Eustis).

Army Installations	IPN	SPPN	ISN*	GSU**	AEDC	APC-E***	DISA DECC

*** APC-E: Four CONUS APC-Es will transition from AEDCs no later than 2025.

TABLE 2: SCHEDULE OF DATA CENTER CLOSURE BY COMMAND OR PROPONENT

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
COMMAND/PROPONENT: AMC						
295	APGD_MD_AMC_04	Aberdeen Proving Ground - AMSAA	AMC	Aberdeen Proving Ground	IPN	2Q16
732	FBRG_NC_AMC_03	Directorate of Logistics Bragg 4-2843	AMC	Fort Bragg	IPN	4Q16
736	FBRG_NC_AMC_07	Directorate of Logistics Bragg F-3040	AMC	Fort Bragg	Server	4Q16
737	FBRG_NC_AMC_08	Directorate of Logistics Bragg M-8139	AMC	Fort Bragg	Server	4Q16
1061	FCRS_CO_AMC_03	Directorate of Logistics AOAP Lab	AMC	Fort Carson	IPN	4Q16
1153	IAAP_IA_AMC_01	Iowa Army Ammunition Plant (IAAP)	AMC	Iowa Army Ammunition Plant	Server	4Q16
1154	LCAP_MO_AMC_01	Lake City Army Ammunition Plant (LCAAP)	AMC	Lake City Army Ammunition Plant	IPN	4Q16
1945	FBRG_NC_AMC_10	U.S. Army Security Assistance Command (USASAC) Security Assistance Training Management Organization (SATMO) Ft. Bragg Data Center	AMC	Fort Bragg	IPN	4Q16
7	RDST_AL_AMC_01	DC - Redstone-LOGSA- Sparkman Center	AMC	Redstone Arsenal	IPN	4Q17
465	PCTA_NJ_AMC_03	EFP-HORTS - Explosively Formed Penetrators - Highly Organized Research/Technology System	AMC	Picatinny Arsenal	SPPN	4Q17
642	FRKR_AL_AMC_01	ACLC- Building 1110	AMC	Fort Rucker	IPN	4Q17
938	FRKR_AL_AMC_05	AMC Data Center Hanchey	AMC	Fort Rucker	IPN	4Q17
1077	PCTA_NJ_AMC_05	METC Fuze and Precision Armaments Research Lab	AMC	Picatinny Arsenal	SPPN	4Q17
1116	PCTA_NJ_AMC_07	METC Warheads Analysis and Evaluation Research Lab UNCLASS	AMC	Picatinny Arsenal	SPPN	4Q17
1124	RILA_IL_AMC_03	ECBC Data Center	AMC	Rock Island Arsenal	SPPN	3Q18

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
4	FRKR_AL_AMC_06	Software Engineering Center (SEC) - Army Reprogramming Analysis Team - Fort Rucker Information System	AMC	Fort Rucker	SPPN	4Q18
17	FHCH_AZ_AMC_01	CSLA Mission - Unique IT Services Center	AMC	Fort Huachuca	IPN	4Q18
72	CAAA_IN_AMC_01	Crane Army Ammunition Activity Installation Processing Nodes 3373	AMC	Crane Army Ammunition Activity	IPN	4Q18
115	STLS_MO_AMC_01	SEC St. Louis Data Center	AMC	SEC St. Louis	SPPN	4Q18
282	FSIL_OK_AMC_01	Fires Software Engineering Division Unclassified Software Development	AMC	Fort Sill	SPPN	4Q18
291	FHOD_TX_AMC_01	Central Technical Support Facility Data Center	AMC	Fort Hood	IPN	4Q18
311	APGD_MD_AMC_05	SEC - Integrated Satellite Communications Lab	AMC	Aberdeen Proving Ground	SPPN	4Q18
325	FHCH_AZ_AMC_02	SEC - Intelligence Fusion Systems-Greely Lab	AMC	Fort Huachuca	SPPN	4Q18
381	PCTA_NJ_AMC_02	Armament SEC Integration Lab	AMC	Picatinny Arsenal	SPPN	4Q18
464	FHCH_AZ_AMC_03	SEC - Intelligence Fusion Systems-Ragatz Lab	AMC	Fort Huachuca	SPPN	4Q18
485	APGD_MD_AMC_07	SEC - C3T Directorate MCD Software Development Lab	AMC	Aberdeen Proving Ground	SPPN	4Q18
486	APGD_MD_AMC_08	SEC - Contingency Communications Laboratory	AMC	Aberdeen Proving Ground	SPPN	4Q18
488	APGD_MD_AMC_10	SEC - Key Management Systems Lab	AMC	Aberdeen Proving Ground	SPPN	4Q18
489	APGD_MD_AMC_11	SEC - Network Management Lab	AMC	Aberdeen Proving Ground	SPPN	4Q18
490	APGD_MD_AMC_12	SEC - Integrated Tactical Communications Lab	AMC	Aberdeen Proving Ground	SPPN	4Q18
492	APGD_MD_AMC_14	SEC - Army Reprogramming Analysis Team Laboratory	AMC	Aberdeen Proving Ground	SPPN	4Q18
494	APGD_MD_AMC_16	SEC - Integrated Sensors Lab	AMC	Aberdeen Proving Ground	SPPN	4Q18
495	APGD_MD_AMC_17	SEC - Mission Equipment Support Branch Lab	AMC	Aberdeen Proving Ground	SPPN	4Q18

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
497	FLEE_VA_AMC_01	SEC - Lee Functional Processing Center	AMC	Fort Lee	IPN	4Q18
499	APGD_MD_AMC_20	SEC - Software Assurance Laboratory	AMC	Aberdeen Proving Ground	SPPN	4Q18
500	APGD_MD_AMC_21	SEC - Enterprise Solutions Directorate - Aberdeen Development Lab	AMC	Aberdeen Proving Ground	SPPN	4Q18
501	APGD_MD_AMC_22	SEC - Test Tools Lab	AMC	Aberdeen Proving Ground	SPPN	4Q18
502	APGD_MD_AMC_23	SEC - Army Net Centric Data Strategy Center of Excellence Lab	AMC	Aberdeen Proving Ground	SPPN	4Q18
504	APGD_MD_AMC_24	SEC - Aberdeen Proving Ground Development Lab	AMC	Aberdeen Proving Ground	SPPN	4Q18
505	APGD_MD_AMC_25	SEC - Aberdeen Proving Ground Classified Lab	AMC	Aberdeen Proving Ground	SPPN	4Q18
507	FSIL_OK_AMC_03	Fires Software Engineering Division Classified Software Development CRN	AMC	Fort Sill	SPPN	4Q18
531	WRRN_MI_AMC_02	TARDEC DREN	AMC	Detroit Arsenal	SPPN	4Q18
702	FHCH_AZ_AMC_10	CSLA - EKMS Data Center	AMC	Fort Huachuca	SPPN	4Q18
801	FLEE_VA_AMC_02	SEC - SPS Lab	AMC	Fort Lee	SPPN	4Q18
809	CHES_VA_AMC_03	SEC Lee LOG FANS - Logistic Domain Federated Net-Centric Site	AMC	Commercial Space - Leased Facility/Army Operated	SPPN	4Q18
842	FHCH_AZ_AMC_11	FHCH_AZ_AMC_New_12 (CAISI)	AMC	Fort Huachuca	SPPN	4Q18
843	FHCH_AZ_AMC_12	FHCH_AZ_AMC_New_13 (TROJAN)	AMC	Fort Huachuca	SPPN	4Q18
848	FHCH_AZ_AMC_17	ISEC Consolidated Labs Huachuca	AMC	Fort Huachuca	SPPN	4Q18
889	APGD_MD_AMC_40	APGD_MD_AMC_6010_203	AMC	Aberdeen Proving Ground	SPPN	4Q18
948	WRRN_MI_AMC_03	TACOM Cost and Systems Analysis - Secure Defense Research Engineering Network	AMC	Detroit Arsenal	SPPN	4Q18
956	FHOD_TX_AMC_04	Central Technical Support Facility - TFN	AMC	Fort Hood	SPPN	4Q18
1140	FPLK_LA_AMC_06	FPLK_LA_ASP 4101	AMC	Fort Polk	IPN	4Q18

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
1627	RDST_AL_AMC_07	USASAC Data Center	AMC	Redstone Arsenal	IPN	4Q18
1912	NCAD_PA_AMC_01	USASAC-NC-Unclassified DC	AMC	New Cumberland Army Depot	IPN	4Q18
1913	NCAD_PA_AMC_02	USASAC Classified DC	AMC	New Cumberland Army Depot	IPN	4Q18
1927	BGRM_AF_AMC_01	401st Army Field Support Battalion, Afghanistan S6 - Conex #35939A	AMC	BAGRAM AIR FIELD	IPN	4Q18
1921	COLB_DE_AMC_01	ASC Coleman	AMC	Coleman Barracks	IPN	4Q20
15	PNBA_AR_AMC_01	Pine Bluff Arsenal Data Center	AMC	Pine Bluff Arsenal	IPN	4Q21
25	SRAD_CA_AMC_01	Data Center Sierra Building 51	AMC	Sierra Army Depot	IPN	4Q21
91	BGAD_KY_AMC_01	Data Center - BGAD_DC_01	AMC	Blue Grass Army Depot	IPN	4Q21
136	HWAD_NV_AMC_01	HWAD NIPRNET	AMC	Hawthorne Army Depot	IPN	4Q21
141	WTVA_NY_AMC_01	Watervliet Arsenal Data Center	AMC	Watervliet Arsenal	IPN	4Q21
149	MAAP_OK_AMC_01	MAAPEN - IMA	AMC	McAlester AAP	IPN	4Q21
156	LTKY_PA_AMC_01	Letterkenny DOIM	AMC	Letterkenny Army Depot	IPN	4Q21
173	RRAD_TX_AMC_01	RRAD184DC	AMC	Red River Army Depot	IPN	4Q21
176	TOOL_UT_AMC_01	Tooele Enterprise NIPRNET	AMC	Tooele Army Depot	IPN	4Q21
245	PUBL_CO_AMC_01	Pueblo Data Center	AMC	Pueblo Chemical Depot	IPN	4Q21
727	CAFB_SC_AMC_01	Army Strategic Logistics Activity Charleston	AMC	Charleston Air Force Base	IPN	4Q21
807	CHES_VA_AMC_01	SEC - HSIF Integration Ghosting	AMC	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
1356	MTSP_NC_AMC_01	Military Ocean Terminal Sunny Point	AMC	Sunny Point	IPN	4Q21
2	ANAD_AL_AMC_01	Anniston DOIM Computer Room	AMC	Anniston Army Depot	IPN	4Q22
163	CCAD_TX_AMC_01	CCAD SITE 1	AMC	Corpus Christi Army Depot	IPN	4Q22
158	TBYA_PA_AMC_01	Tobyhanna DOIM Computer Room	AMC	Tobyhanna Army Depot	IPN	4Q23

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
COMMAND/PROPONENT: ARCENT						
242	CARJ_KW_CEN_01	ARCENT Forward (Arifjan)	ARCENT	Camp Arifjan	IPN	3Q16
930	SHAF_SC_CEN_01	Data Center Shaw AFB USARCENT	ARCENT	Shaw AFB	IPN	4Q18
COMMAND/PROPONENT: ASA (ALT)						
202	FBLV_VA_ALT_03	Army Knowledge Online (AKO) Primary Site One (PS1)	ASA (ALT)	Fort Belvoir	IPN	4Q17
63	RILA_IL_ALT_02	MMCS Server Room	ASA (ALT)	Rock Island Arsenal	IPN	4Q18
696	APGD_MD_ALT_02	PEOC3T Tactical System Integration Facility	ASA (ALT)	Aberdeen Proving Ground	SPPN	4Q18
1561	CPRK_CA_ALT_01	Distributed Learning Systems	ASA (ALT)	Camp Parks	SPPN	4Q18
32	ORLD_FL_ALT_01	PEO STRI - Research Commons Building	ASA (ALT)	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
1563	FHLT_CA_ALT_01	Digital Training Facility DLS	ASA (ALT)	Fort Hunter Liggett	SPPN	4Q24
207	RFAA_VA_ALT_01	Data Center Acquisition Logistics and Technology Enterprise Systems and Services	ASA (ALT)	Radford Army Ammunition Plant	IPN	TBD
COMMAND/PROPONENT: ATEC						
260	FHOD_TX_ATC_01	Data Center - USAOTC	ATEC	Fort Hood	IPN	4Q16
701	RDST_AL_ATC_02	RTCHQ Data Center LAB (COOP Site)	ATEC	Redstone Arsenal	SPPN	4Q16
299	APGD_MD_ATC_04	B 400 Rm 128	ATEC	Aberdeen Proving Ground	IPN	1Q17
301	APGD_MD_ATC_06	B 436 Rm 116c	ATEC	Aberdeen Proving Ground	SPPN	1Q17
264	FBLS_TX_ATC_01	ADATDNET	ATEC	Fort Bliss	SPPN	4Q17
266	FSIL_OK_ATC_01	FSTDNET	ATEC	Fort Sill	SPPN	4Q17
268	FBRG_NC_ATC_01	ABNSOTDNet	ATEC	Fort Bragg	SPPN	4Q17
700	HNVL_AL_ATC_02	RTC HPC Lab	ATEC	Redstone Arsenal	SPPN	2Q18
305	FHCH_AZ_ATC_03	TDDN-DC	ATEC	Fort Huachuca	SPPN	4Q18

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
397	FHOD_TX_ATC_02	TTEC	ATEC	Fort Hood	SPPN	4Q18
398	FGRY_AK_ATC_01	Bolio Lake	ATEC	Fort Greely	SPPN	4Q18
422	WSMR_NM_ATC_24	CRCC - Cox Range Control Center	ATEC	White Sands Missile Range	SPPN	4Q18
441	WSMR_NM_ATC_43	EDSR Development Server	ATEC	White Sands Missile Range	SPPN	4Q18
656	RDST_AL_ATC_01	RTC FTCC	ATEC	Redstone Arsenal	SPPN	4Q18
870	HNVL_AL_ATC_03	RTC EOSFEL	ATEC	Redstone Arsenal	SPPN	4Q18
873	RDST_AL_ATC_04	RTC Electromagnetic Lab	ATEC	Redstone Arsenal	SPPN	4Q18
983	FLCH_VA_ATC_01	IMAT-DC	ATEC	Commercial Space - Leased Facility/Army Operated	SPPN	4Q18
412	WSMR_NM_ATC_15	Building 123 Bay Area	ATEC	White Sands Missile Range	IPN	1Q20
273	HNVL_AL_ATC_01	RTCHQ Data Center LAB	ATEC	Redstone Arsenal	SPPN	4Q20
723	RDST_AL_ATC_03	RTC AVSTIL	ATEC	Redstone Arsenal	SPPN	4Q20
258	YPGR_AZ_ATC_06	YPG-ROC-DC	ATEC	Yuma Proving Ground	IPN	4Q21
303	WSMR_NM_ATC_01	WSMR-DOIM	ATEC	White Sands Missile Range	IPN	4Q23
849	FHCH_AZ_ATC_04	FHCH IEWTD	ATEC	Fort Huachuca	SPPN	4Q24
922	FHOD_TX_ATC_03	IMASE Simulation and Scoring Subsystem	ATEC	Fort Hood	SPPN	4Q24
COMMAND/PROPONENT: AWC						
153	CRLB_PA_AWC_01	CSLSIPR	AWC	Carlisle Barracks	SPPN	4Q24
COMMAND/PROPONENT: DAIG						
1978	FBLV_VA_AIG_01	IGNET-Belvoir	DAIG	Fort Belvoir	SPPN	4Q22
COMMAND/PROPONENT: DUSA						
22	FFLD_CA_DUS_01	Army Data Center Fairfield - Enclave	DUSA	NSLC Pacific	SPPN	4Q18

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
COMMAND/PROPONENT: EUCOM						
1254	PCHB_DE_EUC_01	USEUCOM Data Center	EUCOM	Patch Barracks	IPN	2Q18
COMMAND/PROPONENT: EUSA						
628	YONG_KR_8TH_01	Installation Processing Node CP TANGO	EUSA	USAG Yongsan	IPN	2Q18
COMMAND/PROPONENT: FORSCOM						
252	FBRG_NC_FOR_01	APC Bragg	FORSCOM	Fort Bragg	IPN	4Q18
1142	FPLK_LA_FOR_02	FPLK_LA_JRTC NOC	FORSCOM	Fort Polk	IPN	4Q18
1143	FPLK_LA_FOR_03	FPLK_LA_RNG45	FORSCOM	Fort Polk	SPPN	4Q24
1858	FBLS_TX_FOR_03	Division West Logical Data Center (5th AR FBTX)	FORSCOM	Fort Bliss	SPPN	4Q24
COMMAND/PROPONENT: HQDA COS						
247	FRKR_AL_HQD_01	U.S. Army Combat Readiness /Safety Center Data Center	HQDA CoS	Fort Rucker	SPPN	4Q18
COMMAND/PROPONENT: HQDA G-1						
827	KSLT_DE_HG1_01	CHRA Europe Region Processing Center	HQDA G-1	USAG Kaiserslautern	IPN	2Q17
69	RILA_IL_HG1_01	Army Civilian Data Center	HQDA G-1	Rock Island Arsenal	IPN	4Q17
74	INDY_IN_HG1_03	HRC-Recruiting Services Network-Installation Processing Node	HQDA G-1	DFAS Building 1 Indianapolis IN	IPN	4Q18
756	ALBQ_NM_HG1_01	Albuquerque Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
758	AMRL_TX_HG1_01	Amarillo Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
759	ANCR_AK_HG1_01	Anchorage Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
760	FGIL_GA_HG1_01	Atlanta Military Entrance Processing Station	HQDA G-1	Fort Gillem	IPN	4Q18
761	FGMD_MD_HG1_01	Baltimore Military Entrance Processing Station	HQDA G-1	Fort George G. Meade	IPN	4Q18
762	GLJN_WV_HG1_01	Beckley Military Entrance Processing Station	HQDA G-1	Commercial Space -	IPN	4Q18

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
				Leased Facility/Army Operated		
763	BOIS_ID_HG1_01	Boise Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
764	BSTN_MA_HG1_01	Boston Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
765	NFAR_NY_HG1_01	Buffalo Military Entrance Processing Station	HQDA G-1	Niagara Falls Air Reserve Station	IPN	4Q18
766	BUTT_MT_HG1_01	Butte Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
767	CHRL_NC_HG1_01	Charlotte Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
768	DSPL_IL_HG1_01	Chicago Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
769	CLEV_OH_HG1_01	Cleveland Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
770	CLMB_OH_HG1_01	Columbus Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
771	DLLS_TX_HG1_01	Dallas Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
772	DNVR_CO_HG1_01	Denver Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
773	CDGE_IA_HG1_01	Des Moines Military Entrance Processing Station	HQDA G-1	Camp Dodge	IPN	4Q18
774	TROY_MI_HG1_01	Detroit Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
775	ELPS_TX_HG1_01	El Paso Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
776	FARG_ND_HG1_01	Fargo Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
777	FDIX_NJ_HG1_01	Fort Dix Military Entrance Processing Station	HQDA G-1	Fort Dix	IPN	4Q18
778	FJSN_SC_HG1_01	Fort Jackson Military Entrance Processing Station	HQDA G-1	Fort Jackson	IPN	4Q18
779	FLEE_VA_HG1_01	Fort Lee Military Entrance Processing Station	HQDA G-1	Fort Lee	IPN	4Q18
780	MBRG_PA_HG1_01	Harrisburg Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
781	NSPH_HI_HG1_01	Honolulu Military Entrance Processing Station	HQDA G-1	NAVSTA Pearl Harbor	IPN	4Q18
782	HSTN_TX_HG1_01	Houston Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
783	INDY_IN_HG1_02	Indianapolis Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
784	JCSN_MS_HG1_01	Jackson Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
785	JCVL_FL_HG1_01	Jacksonville Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
786	KSCY_MO_HG1_01	Kansas City Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
787	KNVL_TN_HG1_01	Knoxville Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
788	LNNG_MI_HG1_01	Lansing Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
789	LTRK_AR_HG1_01	Little Rock Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
790	ELSG_CA_HG1_01	Los Angeles Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
791	LSVL_KY_HG1_01	Louisville Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
792	MMPH_TN_HG1_01	Memphis Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
793	MIAM_FL_HG1_01	Miami Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
794	MILW_WI_HG1_01	Milwaukee Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
795	MPLS_MN_HG1_01	Minneapolis Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
796	MTGM_AL_HG1_01	Montgomery Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
797	NSVL_TN_HG1_01	Nashville Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
798	KNBG_LA_HG1_01	New Orleans Military Entrance Processing Station	HQDA G-1	Naval Air Station Joint Reserve Base, New Orleans	IPN	4Q18
799	FHAM_NY_HG1_01	New York Military Entrance Processing Station	HQDA G-1	USAG Fort Hamilton	IPN	4Q18
800	OKCY_OK_HG1_01	Oklahoma City Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
816	PITB_PA_HG1_01	Pittsburgh Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
817	PTLD_ME_HG1_01	Portland (ME) Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
818	PTLD_OR_HG1_01	Portland (OR) Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
819	SCRM_CA_HG1_01	Sacramento Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
820	WVCY_UT_HG1_01	Salt Lake City Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
821	FSAM_TX_HG1_01	San Antonio Military Entrance Processing Station	HQDA G-1	Fort Sam Houston	IPN	4Q18
822	SNDG_CA_HG1_01	San Diego Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
823	MTVW_CA_HG1_01	San Jose Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
824	FBCH_PR_HG1_01	San Juan Military Entrance Processing Station (DOD)	HQDA G-1	Fort Buchanan	IPN	4Q18
825	STTL_WA_HG1_01	Seattle Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
826	SHPT_LA_HG1_01	Shreveport Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
828	SXFL_SD_HG1_01	Sioux Falls Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
829	SPKN_WA_HG1_01	Spokane Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
830	WAFB_MA_HG1_01	Springfield Military Entrance Processing Station	HQDA G-1	Westover Air Force Reserve Base	IPN	4Q18
831	STLS_MO_HG1_02	St. Louis Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
832	HANG_NY_HG1_01	Syracuse Military Entrance Processing Station	HQDA G-1	Hancock Field Air National Guard Base	IPN	4Q18
833	TAMP_FL_HG1_01	Tampa Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
1953	RLGH_NC_HG1_02	Raleigh Military Entrance Processing Station	HQDA G-1	Great Lakes Naval Training Center	IPN	4Q18
1954	OMAH_NE_HG1_01	Omaha Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
1955	PHNX_AZ_HG1_01	Phoenix Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
86	FKNX_KY_HG1_01	Data Center - Human Resources Command (DC-HRC)	HQDA G-1	Fort Knox	IPN	2Q21
749	GLTC_IL_HG1_01	HQ USMEPCOM Enterprise Data Center	HQDA G-1	Great Lakes Naval Training Center	IPN	4Q21
750	ALBY_NY_HG1_01	USMEPCOM Albany Military Entrance Processing Station	HQDA G-1	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
COMMAND/PROPONENT: HQDA G-2						
536	CLSP_CO_HG2_01	ARSTRAT GEOINT DIV Computer Room	HQDA G-2	Peterson AFB	SPPN	4Q16
COMMAND/PROPONENT: HQDA G-3						
466	FBLS_TX_HG3_01	G3 MTC - Fort Bliss	HQDA G-3	Fort Bliss	SPPN	4Q24

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
467	FBRG_NC_HG3_01	G3 MTC - Fort Bragg	HQDA G-3	Fort Bragg	SPPN	4Q24
468	FCBL_KY_HG3_01	G3 MTC - Fort Campbell	HQDA G-3	Fort Campbell	SPPN	4Q24
469	FCRS_CO_HG3_01	G3 MTC - Fort Carson (Legacy)	HQDA G-3	Fort Carson	SPPN	4Q24
470	FDRM_NY_HG3_01	G3 MTC - Fort Drum	HQDA G-3	Fort Drum	SPPN	4Q24
471	FHOD_TX_HG3_01	G3 MTC-Fort Hood	HQDA G-3	Fort Hood	SPPN	4Q24
472	FKNX_KY_HG3_01	G3 MTC - Fort Knox	HQDA G-3	Fort Knox	SPPN	4Q24
473	JBLM_WA_HG3_01	G3 MTC - Joint Base Lewis-McChord	HQDA G-3	Joint Base Lewis-McChord	SPPN	4Q24
474	FPLK_LA_HG3_01	G3 MTC - Fort Polk	HQDA G-3	Fort Polk	SPPN	4Q24
475	JBER_AK_HG3_01	G3 MTC - Joint Base Elmendorf-Richardson (Legacy)	HQDA G-3	Fort Richardson	SPPN	4Q24
476	FRLY_KS_HG3_01	G3 MTC - Fort Riley	HQDA G-3	Fort Riley	SPPN	4Q24
478	FSAM_TX_HG3_02	G3 MTC -Joint Base San Antonio	HQDA G-3	Fort Sam Houston	SPPN	4Q24
479	FSIL_OK_HG3_01	G3 MTC - Fort Sill (Legacy)	HQDA G-3	Fort Sill	SPPN	4Q24
480	FSTW_GA_HG3_01	G3 MTC - Fort Stewart (Legacy)	HQDA G-3	Fort Stewart	SPPN	4Q24
481	FWNW_AK_HG3_01	G3 MTC - Fort Wainwright	HQDA G-3	Fort Wainwright	SPPN	4Q24
482	CZMA_JP_HG3_01	G3 MTC - Sagami Japan	HQDA G-3	Camp Zama	SPPN	4Q24
483	SCOB_HI_HG3_01	G3 MTC - Schofield Barracks	HQDA G-3	Schofield Barracks	SPPN	4Q24
538	SHAF_SC_HG3_01	G3 MTC - Shaw AFB	HQDA G-3	Shaw AFB	SPPN	4Q24
578	YONG_KR_HG3_01	G3 MTC - KBSC	HQDA G-3	USAG Yongsan	SPPN	4Q24
710	EHRC_TX_HG3_01	G3 MTC - 1/75th MCTD Houston	HQDA G-3	63rd Regional Support Command	SPPN	4Q24
711	FDIX_NJ_HG3_01	G3 MTC - 2/75th MCTD Fort Dix	HQDA G-3	Fort Dix	SPPN	4Q24
712	ARLH_IL_HG3_01	G3 MTC - 3/75th MCTD Arlington Heights	HQDA G-3	88th Regional Support Command	SPPN	4Q24
713	BRHM_AL_HG3_01	G3 MTC - 4/75th MCTD Birmingham	HQDA G-3	81st Regional Support Command	SPPN	4Q24
714	CPRK_CA_HG3_01	G3 MTC - 5/75th MCTD Camp Parks	HQDA G-3	Camp Parks	SPPN	4Q24

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
COMMAND/PROPONENT: HQDA G-4-						
708	FDRM_NY_HG4_03	LRC DRUM SAMS-I(E)	HQDA G-4	Fort Drum	Server	4Q16
733	FBRG_NC_HG4_03	DOL Bragg W-1335	HQDA G-4	Fort Bragg	Server	4Q16
901	APGD_MD_HG4_03	APGD_MD_DOL_4302_3	HQDA G-4	Aberdeen Proving Ground	Server	4Q16
959	FHOD_TX_HG4_02	Directorate of Logistics DRRF B25015	HQDA G-4	Fort Hood	IPN	4Q16
1102	JBLM_WA_HG4_01	JBLM DOL TC-AIMS II 9614	HQDA G-4	Joint Base Lewis-McChord	IPN	4Q16
1242	FBNG_GA_HG4_02	FBNG DOL SAMS 2411	HQDA G-4	Fort Benning	IPN	4Q16
1331	FGMD_MD_HG4_01	TCAIMS Data Center	HQDA G-4	Fort George G. Meade	IPN	4Q16
1626	FCBL_KY_HG4_03	Coordinate Transport Operations	HQDA G-4	Fort Campbell	IPN	4Q16
962	FHOD_TX_HG4_05	Directorate of Logistics Building 88037	HQDA G-4	Fort Hood	IPN	1Q17
1063	FCRS_CO_HG4_04	DOL SAMS - IE 8000	HQDA G-4	Fort Carson	IPN	1Q17
1104	JBLM_WA_HG4_03	JBLM DOL SAMS 9580	HQDA G-4	Joint Base Lewis-McChord	IPN	1Q17
155	CHBG_PA_HG4_01	LMP Data Center	HQDA G-4	CSC Chambersburg	IPN	2Q17
179	STLS_MO_HG4_01	LMP COOP	HQDA G-4	SEC St. Louis	IPN	2Q17
1136	FPLK_LA_HG4_01	FPLK DOL SAMS-IE 4386	HQDA G-4	Fort Polk	IPN	3Q17
1297	FKNX_KY_HG4_02	FKNX DOL SAMS-IE 2778	HQDA G-4	Fort Knox	IPN	3Q17
1389	FMCY_WI_HG4_01	FMCY DOL SAAS/WSUS 209	HQDA G-4	Fort McCoy	IPN	3Q17
1554	POMR_CA_HG4_01	Fort Ord SAMS-E	HQDA G-4	Presidio of Monterey	IPN	3Q17
703	FDRM_NY_HG4_01	LRC DRUM SAAS-MOD	HQDA G-4	Fort Drum	Server	1Q18
734	FBRG_NC_HG4_02	DOL Bragg 5003	HQDA G-4	Fort Bragg	Server	1Q18
900	APGD_MD_HG4_02	APGD_MD_DOL_4302_10B	HQDA G-4	Aberdeen Proving Ground	Server	1Q18
960	FHOD_TX_HG4_03	Directorate of Logistics Ammunition Supply Point Building 92076	HQDA G-4	Fort Hood	IPN	1Q18
1064	FCRS_CO_HG4_05	DOL SAAS-MOD 9370	HQDA G-4	Fort Carson	IPN	1Q18

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
1095	JBLM_WA_HG4_05	JBLM DOL SAAS-MOD 1093	HQDA G-4	Joint Base Lewis-McChord	IPN	1Q18
1105	JBLM_WA_HG4_04	JBLM DOL SAAS-MOD M0001	HQDA G-4	Joint Base Lewis-McChord	IPN	1Q18
1155	RILA_IL_HG4_01	RILA DOL SAAS-MOD 154	HQDA G-4	Rock Island Arsenal	IPN	1Q18
1244	FBNG_GA_HG4_04	FBNG DOL SAAS-MOD 6000	HQDA G-4	Fort Benning	IPN	1Q18
1296	FKNX_KY_HG4_01	FKNX DOL 3075	HQDA G-4	Fort Knox	IPN	1Q18
1362	FLVN_KS_HG4_02	FLVN DOL SAAS-MOD 341	HQDA G-4	Fort Leavenworth	IPN	1Q18
1601	FCBL_KY_HG4_02	Standard Army Ammunition System Modernization (SAAS-MOD)	HQDA G-4	Fort Campbell	IPN	1Q18
1910	MNSS_VA_HG4_01	Data Center-PDAMIS-RFITV-LMCO	HQDA G-4	Commercial Space - Outsourced	SPPN	4Q18
1390	FMCY_WI_HG4_02	FMCY IMMA 200	HQDA G-4	Fort McCoy	IPN	4Q19
704	FDRM_NY_HG4_02	AFMA DRUM ULLS-AE	HQDA G-4	Fort Drum	Server	4Q22
963	FHOD_TX_HG4_06	Directorate of Logistics Building 7012	HQDA G-4	Fort Hood	IPN	4Q22
1011	FSTW_GA_HG4_01	ULLS-A(E) Hunter AAF	HQDA G-4	Hunter AAF	IPN	4Q22
1065	FCRS_CO_HG4_06	DOL ULLS-A 9604	HQDA G-4	Fort Carson	IPN	4Q22
1238	FBNG_GA_HG4_01	ACLC Benning Airfield ULLS-A(E)	HQDA G-4	Fort Benning	IPN	4Q22
1584	FCBL_KY_HG4_01	Regional Aviation Sustainment Maintenance - C (RASM-C)	HQDA G-4	Fort Campbell	IPN	4Q22
284	NCLD_PA_HG4_01	LIA Data Center New Cumberland	HQDA G-4	Defense Distribution Services Pennsylvania	IPN	4Q24
COMMAND/PROPONENT: HQDA G-8						
680	FBLV_VA_HG8_01	Center for Army Analysis Data Center	HQDA G-8	Fort Belvoir	SPPN	4Q24
1629	FBLV_VA_HG8_02	ARMY MODELING AND SIMULATION OFFICE - SYNTHETIC TRAINING ENVIRONMENT	HQDA G-8	Fort Belvoir	SPPN	4Q24
COMMAND/PROPONENT: IMCOM						
429	WSMR_NM_IMC_01	FMWR Data Center	IMCOM	White Sands Missile Range	IPN	2Q16

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
1302	FKNX_KY_IMC_02	FKNX MWR DC	IMCOM	Fort Knox	IPN	2Q16
667	FBLS_TX_IMC_09	FBLS_TX_DPW_622	IMCOM	Fort Bliss	SPPN	3Q16
958	FLWD_MO_IMC_01	MWR - Building 470	IMCOM	Fort Leonard Wood	Server	3Q16
966	FGRD_GA_IMC_02	FGRD_GA_DPW 14600	IMCOM	Fort Gordon	IPN	3Q16
973	FGRD_GA_IMC_06	FGRD_GA_DH 33720	IMCOM	Fort Gordon	IPN	3Q16
907	APGD_MD_IMC_11	APGD_MD_MWR_B2314	IMCOM	Aberdeen Proving Ground	Server	4Q16
1117	JBLM_WA_IMC_10	JBLM_WA_DPW Building	IMCOM	Joint Base Lewis-McChord	IPN	4Q16
1377	FLEE_VA_IMC_02	FLEE IMC 6222	IMCOM	Fort Lee	IPN	4Q16
1578	FCBL_TN_IMC_01	DPTMS Multimedia / Visual Information Service Center (MVISC)	IMCOM	Fort Campbell	IPN	4Q16
1583	FCBL_TN_IMC_02	FCBL MWR	IMCOM	Fort Campbell	IPN	4Q16
1585	FCBL_TN_IMC_03	Glenn H. English Army Education Center, Automation Office	IMCOM	Fort Campbell	IPN	4Q16
1857	RMTA_CO_IMC_01	RMA_CO_Enterprise_Services	IMCOM	Rocky Mountain Arsenal	IPN	4Q16
739	FBRG_NC_IMC_08	IMCOM Directorate of Plans, Training, Mobilization, and Security Range Control A-1308	IMCOM	Fort Bragg	Server	3Q18
955	FHOD_TX_IMC_02	Education Services	IMCOM	Fort Hood	SPPN	4Q18
1345	FJSN_SC_IMC_06	FJSN CDC 4581	IMCOM	Fort Jackson	SPPN	4Q18
1272	FLWD_MO_IMC_02	Visual Information Center	IMCOM	Fort Leonard Wood	IPN	4Q21
120	FBRG_NC_INS_02	GISA Data Center	INSCOM	Fort Bragg	SPPN	3Q16
COMMAND/PROPONENT: INSCOM						
463	DMST_DE_INS_01	66th MI Brigade Data Center	INSCOM	Dagger Complex	SPPN	3Q16
41	FGRD_GA_INS_01	Luketina Hall	INSCOM	Fort Gordon	SPPN	4Q16
277	FSAM_TX_INS_01	470th MI BDE Computer Equipment Room (CER)	INSCOM	Fort Sam Houston	SPPN	4Q16
1972	FGMD_MD_INS_05	ACO (Army Cryptologic Office)	INSCOM	Fort George G. Meade	SPPN	4Q16

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
1973	FGMD_MD_INS_06	780th MI BDE	INSCOM	Fort George G. Meade	SPPN	4Q16
1974	FGMD_MD_INS_07	AFSC	INSCOM	Fort George G. Meade	SPPN	4Q16
1975	WBDN_DE_INS_02	1st MI BN	INSCOM	Clay Kaserne	SPPN	4Q16
1976	HMPY_KR_INS_02	532nd MI BN	INSCOM	Camp Humphreys	SPPN	4Q16
1977	FSFT_HI_INS_02	205th MI BN	INSCOM	Fort Shafter	SPPN	4Q16
271	SCOB_HI_INS_01	500 MI Brigade, HQ	INSCOM	Schofield Barracks	SPPN	2Q17
278	YONG_KR_INS_01	501st MI North	INSCOM	USAG Yongsan	SPPN	2Q17
281	HMPY_KR_INS_01	Network Operations Center Korea (NOC-K)	INSCOM	Camp Humphreys	SPPN	2Q17
316	CZMP_JP_INS_01	441st-500th MI Brigade, HQ	INSCOM	Camp Zama	SPPN	2Q17
323	FBLS_TX_INS_01	204th MI BN Data Center	INSCOM	Fort Bliss	SPPN	2Q17
279	FGMD_MD_INS_01	902d HQ S6 Data Center	INSCOM	Fort George G. Meade	SPPN	4Q22
280	FGMD_MD_INS_04	704th MI Brigade, HQ	INSCOM	Fort George G. Meade	SPPN	4Q22
293	FGMD_MD_INS_03	Army Operations Group	INSCOM	Fort George G. Meade	SPPN	4Q22
COMMAND/PROPONENT: NETCOM						
1347	DGWY_UT_NEC_03	NEC SIPR Vault	NETCOM	Dugway Proving Ground	IPN	4Q15
113	FLWD_MO_NEC_01	DC-FLWNEC	NETCOM	Fort Leonard Wood	IPN	1Q16
932	FSAM_TX_NEC_05	FSAM_TX_NEC_05	NETCOM	Fort Sam Houston	IPN	1Q16
111	FLWD_MO_NEC_02	DC-FLWNEC2	NETCOM	Fort Leonard Wood	IPN	2Q16
10	FRKR_AL_NEC_01	Ft Rucker NIPR Data Center	NETCOM	Fort Rucker	IPN	4Q16
19	FHCH_AZ_NEC_02	Data Center - Ft Huachuca NEC SIPRNET, DC - Huachuca NEC SIPRNET	NETCOM	Fort Huachuca	IPN	4Q16
64	RILA_IL_NEC_01	Data Center-NEC-RIA-103	NETCOM	Rock Island Arsenal	IPN	4Q16
85	FRLY_KS_NEC_03	DC - Riley03 - COMSEC Center	NETCOM	Fort Riley	IPN	4Q16
168	FHOD_TX_NEC_01	Fort Hood NEC 13	NETCOM	Fort Hood	IPN	4Q16
1113	JBLM_WA_NEC_07	JBLM_WA_NEC_POP	NETCOM	Joint Base Lewis-McChord	IPN	4Q16

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
1194	WRRN_MI_NEC_05	FCS - Warren	NETCOM	Detroit Arsenal	IPN	4Q16
1328	FBNG_GA_NEC_11	FBNG NEC Merrill 12	NETCOM	Fort Benning	IPN	4Q16
1348	CLMB_OH_NEC_01	Columbus Army Green Space	NETCOM	DISA DECC Columbus	IPN	4Q16
1354	RDST_AL_NEC_03	RDST Data Center COOP	NETCOM	Redstone Arsenal	IPN	4Q16
1357	TAFB_OK_NEC_01	Oklahoma City DECC Green Space	NETCOM	Tinker AFB	IPN	4Q16
1365	FLVN_KS_NEC_02	FLVN NEC DR 120	NETCOM	Fort Leavenworth	IPN	4Q16
1368	FDTK_MD_NEC_02	FDTK Post HQ NEC 810	NETCOM	Fort Detrick	IPN	4Q16
1386	FMCY_WI_NEC_03	FMCY NEC Back-up 2692	NETCOM	Fort McCoy	IPN	4Q16
1387	FMCY_WI_NEC_04	FMCY NEC S-Backup 2691	NETCOM	Fort McCoy	IPN	4Q16
1525	FDIX_NJ_NEC_03	Fort Dix NEC COOP	NETCOM	Fort Dix	IPN	4Q16
1562	CRBT_CA_NEC_01	Camp Roberts NEC	NETCOM	Camp Roberts	IPN	4Q16
112	FLWD_MO_NEC_03	DC-FLWNEC3	NETCOM	Fort Leonard Wood	IPN	1Q17
160	FJSN_SC_NEC_01	Data Center - USASNEC Fort Jackson	NETCOM	Fort Jackson	IPN	1Q17
240	CARJ_KW_160_01	Arifjan TCF Building 209 Rm 133	NETCOM	Camp Arifjan	IPN	1Q17
241	CARJ_KW_160_02	Arifjan TAC TCF Building T521	NETCOM	Camp Arifjan	IPN	1Q17
837	FHCH_AZ_NEC_06	FHCH_AZ_NEC_New_06	NETCOM	Fort Huachuca	IPN	1Q17
841	FHCH_AZ_NEC_10	FHCH_AZ_NET_New_06 (Greely J&K)	NETCOM	Fort Huachuca	SPPN	1Q17
54	HAAF_GA_NEC_01	DataCenter-HunterAAF-H935	NETCOM	Hunter AAF	IPN	2Q17
192	FEUS_VA_NEC_01	NEC Eustis	NETCOM	Fort Eustis	IPN	2Q17
1374	FRFX_VA_NEC_01	AWRAC	NETCOM	Fort Belvoir	SPPN	2Q17
1351	FJSN_SC_NEC_03	FJSN NEC 4282	NETCOM	Fort Jackson	IPN	3Q17
70	RILA_IL_NEC_05	Data Center-NEC-RIA-South Computer Room	NETCOM	Rock Island Arsenal	IPN	4Q17
90	FKNX_KY_NEC_02	NEC Data Center - Knox	NETCOM	Fort Knox	IPN	4Q17
211	JBLM_WA_NEC_01	Data Center - JBLM 1	NETCOM	Joint Base Lewis-McChord	IPN	1Q18

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
212	JBLM_WA_NEC_02	Data Center - JBLM 2	NETCOM	Joint Base Lewis-McChord	IPN	1Q18
839	FHCH_AZ_NEC_08	FHCH_AZ_NET_New_04 (Greely 1214)	NETCOM	Fort Huachuca	IPN	1Q18
840	FHCH_AZ_NEC_09	FHCH_AZ_NET_New_05 (Greely 1004)	NETCOM	Fort Huachuca	IPN	1Q18
1060	FPLK_LA_NEC_04	Network Enterprise Center-Fort Polk 7840	NETCOM	Fort Polk	IPN	1Q18
1963	FBNG_GA_NEC_12	FBNG NEC B4	NETCOM	Fort Benning	IPN	1Q18
104	FGMD_MD_NEC_01	NEC Fort Meade	NETCOM	Fort George G. Meade	IPN	4Q18
108	WRRN_MI_NEC_02	Data Center SIPR - Warren	NETCOM	Detroit Arsenal	IPN	4Q18
167	FBLS_TX_NEC_02	Fort_Bliss_NEC_B13480	NETCOM	Fort Bliss	IPN	4Q18
187	FBLV_VA_NEC_02	NEC Fort Belvoir - SIPR	NETCOM	Fort Belvoir	IPN	4Q18
308	FHCH_AZ_NET_03	NETCOM G5 EOF	NETCOM	Fort Huachuca	SPPN	4Q18
1107	JBLM_WA_NEC_06	JBLM_WA_NEC_Classroom	NETCOM	Joint Base Lewis-McChord	SPPN	4Q18
94	FDVN_MA_NEC_01	NEC Fort Devens	NETCOM	Devens Reserve Training Area	IPN	4Q20
95	NATK_MA_NEC_01	NEC Natick	NETCOM	Natick Soldier Systems Center	IPN	4Q20
128	FDIX_NJ_NEC_01	NEC Fort Dix	NETCOM	Fort Dix	IPN	4Q20
129	PCTA_NJ_NEC_01	Pica Main Data Center (Bldg 351 Rooms 3 & 35)	NETCOM	Picatinny Arsenal	IPN	4Q20
137	FHAM_NY_NEC_01	Network Enterprise Center - Fort Hamilton	NETCOM	USAG Fort Hamilton	IPN	4Q20
154	CRLB_PA_NEC_01	NEC Carlisle Barracks	NETCOM	Carlisle Barracks	IPN	4Q20
183	FAPH_VA_NEC_01	NEC Fort A.P. Hill	NETCOM	Fort A.P. Hill	IPN	4Q20
199	FMYR_VA_NEC_01	NEC - Fort Myer	NETCOM	Joint Base Myer - Henderson Hall	IPN	4Q20
307	YONG_KR_NET_01	Northern Node	NETCOM	USAG Yongsan	IPN	4Q20
951	FBCH_PR_NEC_01	Fort Buchanan	NETCOM	Fort Buchanan	IPN	4Q20
1	FWNW_AK_NEC_01	Alaska Regional Data Center	NETCOM	Fort Wainwright	IPN	4Q21

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
175	DGWY_UT_NEC_01	NEC-DPG Data Center (formerly DREN Computer Room)	NETCOM	Dugway Proving Ground	IPN	4Q21
314	FGRY_AK_NEC_01	Data Center - Fort Greely	NETCOM	Fort Greely	IPN	4Q21
521	FBLS_TX_NEC_03	Data_Center_B56A	NETCOM	Fort Bliss	IPN	4Q21
923	VCNZ_IT_NEC_01	Migliore Data Center Del Din	NETCOM	Del Din	IPN	4Q21
1503	FHLT_CA_NEC_01	Fort Hunter Liggett NEC 197	NETCOM	Fort Hunter Liggett	IPN	4Q21
1506	CPRK_CA_NEC_01	Camp Parks NEC	NETCOM	Camp Parks	IPN	4Q21
18	FHCH_AZ_NEC_01	Data Center - Ft Huachuca NEC NIPRNET, DC - Huachuca NEC NIPRNET	NETCOM	Fort Huachuca	IPN	4Q22
27	POMR_CA_NEC_01	POM NEC Server Room	NETCOM	Presidio of Monterey	IPN	4Q22
56	FGRD_GA_NEC_01	NEC Fort Gordon	NETCOM	Fort Gordon	IPN	4Q22
65	RILA_IL_NEC_02	159 G5 Server Room	NETCOM	Rock Island Arsenal	IPN	4Q22
77	FLVN_KS_NEC_01	Data Center - Leavenworth NEC	NETCOM	Fort Leavenworth	IPN	4Q22
93	FPLK_LA_NEC_01	Network Enterprise Center-Fort Polk	NETCOM	Fort Polk	IPN	4Q22
96	APGD_MD_NEC_01	Network Enterprise Center Aberdeen Proving Ground	NETCOM	Aberdeen Proving Ground	IPN	4Q22
107	WRRN_MI_NEC_01	Data Center - Warren	NETCOM	Detroit Arsenal	IPN	4Q22
186	FBLV_VA_NEC_01	NEC Fort Belvoir - NIPR	NETCOM	Fort Belvoir	IPN	4Q22
270	FSAM_TX_NEC_04	NEC Data Center FORT SAM HOUSTON Consolidated	NETCOM	Fort Sam Houston	IPN	4Q22
317	FDTK_MD_NEC_01	Fort Detrick NEC	NETCOM	Fort Detrick	IPN	4Q22
318	FLEE_VA_NEC_02	New Data Center-Lee	NETCOM	Fort Lee	IPN	4Q22
924	FLWD_MO_NEC_04	FLWD_MO_NEC_04	NETCOM	Fort Leonard Wood	IPN	4Q22
1151	FJSN_SC_NEC_02	IPN 5615 - USASNEC Fort Jackson	NETCOM	Fort Jackson	IPN	4Q22
1152	FMCY_WI_NEC_02	1454 Main Data Center (new)	NETCOM	Fort McCoy	IPN	4Q22
12	FRKR_AL_NEC_03	Ft Rucker COOP Center	NETCOM	Fort Rucker/Cairns Air Field	IPN	4Q23
23	FIWN_CA_NEC_01	NEC Fort Irwin	NETCOM	Fort Irwin	IPN	4Q23

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
36	FBNG_GA_NEC_01	Data Center Benning NIPR	NETCOM	Fort Benning	IPN	4Q23
62	SCOB_HI_NEC_01	Information Systems Facility	NETCOM	Schofield Barracks	IPN	4Q23
145	USMA_NY_NEC_01	NEC Data Center	NETCOM	USMA West Point	IPN	4Q23
147	FSIL_OK_NEC_01	Fort Sill NEC	NETCOM	Fort Sill	IPN	4Q23
530	JBLM_WA_NEC_04	Data Center - JBLM Yakima	NETCOM	Joint Base Lewis-McChord	IPN	4Q23
46	FSTW_GA_NEC_01	DataCenter-Ft.Stewart-S3	NETCOM	Fort Stewart	IPN	4Q24
59	FSFT_HI_NEC_01	30th Signal NEC Data Center	NETCOM	Fort Shafter	IPN	4Q24
83	FRLY_KS_NEC_01	DC- Riley01 Server Farm	NETCOM	Fort Riley	IPN	4Q24
88	FCBL_KY_NEC_01	NEC DC Fort Campbell	NETCOM	Fort Campbell	IPN	4Q24
138	FDRM_NY_NEC_01	FT Drum NEC Primary	NETCOM	Fort Drum	IPN	4Q24
169	FHOD_TX_NEC_02	Fort Hood NEC 422	NETCOM	Fort Hood	IPN	4Q24
239	CBST_XK_5SG_01	TCF Bondsteel	NETCOM	Camp Bondsteel	IPN	4Q24
522	CASY_QA_NEC_01	Camp As Sayliyah (CAS) Data Center	NETCOM	Camp As Sayliyah	IPN	4Q24
COMMAND/PROPONENT: NGB						
182	FRFX_VA_NGB_01	ARNG WO NOSC	NGB	Commercial Space - Leased Facility/Army Operated	IPN	4Q18
516	ARTN_VA_NGB_01	Arlington Hall Station Installation Processing Node	NGB	Arlington Hall Station	IPN	4Q18
520	NLRK_AR_NGB_02	Professional Education Center - EDU	NGB	Camp Robinson	SPPN	4Q18
699	FBLV_VA_NGB_01	OSAA Facility (IPN)	NGB	Fort Belvoir	IPN	4Q18
519	CDSN_WV_NGB_01	NGB ALT DC	NGB	Camp Dawson	IPN	4Q22
716	FLVN_KS_NGB_01	G3 MTC - ARNG Leavenworth	NGB	Fort Leavenworth	SPPN	4Q24
717	FING_PA_NGB_02	G3 MTC - ARNG Fort Indiantown Gap	NGB	Fort Indiantown Gap Training Site	SPPN	4Q24
718	CDGE_IA_NGB_02	G3 MTC- ARNG Camp Dodge	NGB	Camp Dodge	SPPN	4Q24

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
COMMAND/PROPONENT: OAA						
321	ALXN_VA_OAA_01	Records Management and Declassification Agency	OAA	Fort Belvoir - Humphreys Engineer Center	IPN	3Q18
949	ARTN_VA_OAA_01	Taylor Building Lab	OAA	Commercial Space - Leased Facility/Army Operated	SPPN	4Q18
210	PENT_DC_OAA_01	USAITA Pentagon Data Center	OAA	Pentagon	IPN	4Q19
1412	ALXN_VA_OAA_02	Mark Center Data Center	OAA	Pentagon	IPN	4Q21
1959	OVLD_MO_OAA_01	Army Publishing Directorate Media Distribution Division	OAA	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
COMMAND/PROPONENT: OPMG						
324	CLBG_WV_OPM_01	BIMA Clarksburg Data Center	OPMG	Clarksburg WV	IPN	4Q16
COMMAND/PROPONENT: OTJAG						
1334	FGMD_MD_JAG_01	U.S. Army Claims Server Room	OTJAG	Fort George G. Meade	IPN	2Q16
COMMAND/PROPONENT: SOUTHCOM						
251	STCN_HN_USC_02	Joint Task Force Bravo SIPRNET NOC	SOUTHCOM	Soto Cano Air Base	IPN	2Q17
31	KYWS_FL_USC_01	JIATF-S Data Center	SOUTHCOM	NAS Key West - Truman Annex	IPN	4Q18
1437	BGTA_CO_USC_01	USSOUTHCOM SCO Colombia - 1	SOUTHCOM	American Embassy	IPN	4Q18
1438	BGTA_CO_USC_02	USSOUTHCOM SCO Colombia - 2	SOUTHCOM	American Embassy	IPN	4Q18
1439	BRSL_BR_USC_01	USSOUTHCOM SCO Brazil	SOUTHCOM	American Embassy	IPN	4Q18
1440	BRTN_BB_USC_01	USSOUTHCOM SCO Barbados	SOUTHCOM	American Embassy	IPN	4Q18
1441	BNAR_AR_USC_01	USSOUTHCOM SCO Argentina	SOUTHCOM	American Embassy	IPN	4Q18
1442	CRTG_CO_USC_01	USSOUTHCOM SCO Colombia - 3	SOUTHCOM	American Embassy	IPN	4Q18
1443	BLPN_BZ_USC_01	USSOUTHCOM SCO Belize	SOUTHCOM	American Embassy	IPN	4Q18
1444	SNSV_SV_USC_01	USSOUTHCOM SCO El Salvador	SOUTHCOM	American Embassy	IPN	4Q18

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
1445	GRTW_GY_USC_01	USSOUTHCOM SCO Guyana	SOUTHCOM	American Embassy	IPN	4Q18
1446	GTCY_GT_USC_01	USSOUTHCOM SCO Guatemala	SOUTHCOM	American Embassy	IPN	4Q18
1447	KGTN_JM_USC_01	USSOUTHCOM SCO Jamaica	SOUTHCOM	American Embassy	IPN	4Q18
1448	MNGU_NI_USC_01	USSOUTHCOM SCO Nicaragua	SOUTHCOM	American Embassy	IPN	4Q18
1449	MTRC_PE_USC_01	USSOUTHCOM SCO Peru	SOUTHCOM	American Embassy	IPN	4Q18
1450	CDLC_UY_USC_01	USSOUTHCOM SCO Uruguay	SOUTHCOM	American Embassy	IPN	4Q18
1451	PACY_PA_USC_01	USSOUTHCOM SCO Panama	SOUTHCOM	American Embassy	IPN	4Q18
1452	PRMB_SR_USC_01	USSOUTHCOM SCO Suriname	SOUTHCOM	American Embassy	IPN	4Q18
1453	ASCN_PY_USC_01	USSOUTHCOM SCO Paraguay	SOUTHCOM	American Embassy	IPN	4Q18
1454	PAUP_HT_USC_01	USSOUTHCOM SCO Haiti	SOUTHCOM	American Embassy	IPN	4Q18
1455	QUTO_EC_USC_01	USSOUTHCOM SCO Ecuador	SOUTHCOM	American Embassy	IPN	4Q18
1456	SNJS_CR_USC_01	USSOUTHCOM SCO Costa Rica	SOUTHCOM	American Embassy	IPN	4Q18
1457	SNTG_CL_USC_01	USSOUTHCOM SCO Chile	SOUTHCOM	American Embassy	IPN	4Q18
1458	SNDM_DO_USC_01	USSOUTHCOM SCO Dominican Republic	SOUTHCOM	American Embassy	IPN	4Q18
1459	LPAZ_BO_USC_01	USSOUTHCOM SCO Bolivia	SOUTHCOM	American Embassy	IPN	4Q18
250	STCN_HN_USC_01	Joint Task Force Bravo NIPRNET NOC	SOUTHCOM	Soto Cano Air Base	IPN	4Q21
697	GTMO_CU_USC_01	JTF-GITMO Information Tech	SOUTHCOM	NAVSTA Guantanamo Bay	IPN	4Q21
COMMAND/PROPONENT: TRADOC						
206	NWNW_VA_TRA_01	Training Brain Operations Center (TBOC)	TRADOC	Commercial Space - Leased Facility/Army Operated	SPPN	4Q16
1600	FCBL_KY_TRA_11	MTES LAN	TRADOC	Fort Campbell	SPPN	4Q16
164	FBLS_TX_TRA_01	USASMA -001	TRADOC	Fort Bliss	SPPN	1Q17
637	FRKR_AL_TRA_03	Tactical Training Network	TRADOC	Fort Rucker	IPN	1Q17
664	FBLS_TX_TRA_04	FBLS_TX_TRA_11292_906	TRADOC	Fort Bliss	SPPN	1Q17
1332	FGMD_MD_TRA_01	Asymmetric Warfare Group Data Center	TRADOC	Fort George G. Meade	IPN	1Q17

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
33	AGST_GA_TRA_01	SIT01 - Cobb Hall	TRADOC	Fort Gordon	SPPN	2Q17
544	FGRD_GA_TRA_02	OEMTD Fort Gordon	TRADOC	Fort Gordon	SPPN	2Q17
655	FGRD_GA_TRA_03	Fort Gordon System of Systems Lab	TRADOC	Fort Gordon	SPPN	2Q17
971	FGRD_GA_TRA_05	Information Technology Division	TRADOC	Fort Gordon	SPPN	2Q17
636	FRKR_AL_TRA_10	1st Aviation Brigade	TRADOC	Fort Rucker	IPN	3Q17
134	WSMR_NM_TRA_01	TRAC-WSMR DC	TRADOC	White Sands Missile Range	IPN	4Q17
1240	DHLN_GA_TRA_01	RTB Data Center at GSU Dahlonega	TRADOC	Fort Benning	IPN	4Q17
76	FLVN_KS_TRA_02	BCBLL-BLCSE - Pope Hall	TRADOC	Fort Leavenworth	SPPN	1Q18
78	FLVN_KS_TRA_03	CGSC Server Farm	TRADOC	Fort Leavenworth	SPPN	4Q18
194	FLEE_VA_TRA_01	TRADOC-ALU-ADC001	TRADOC	Fort Lee	SPPN	4Q18
195	FLEE_VA_TRA_02	TRADOC-ALU-ADC002	TRADOC	Fort Lee	SPPN	4Q18
326	FEUS_VA_TRA_02	U.S. Army Aviation Logistics School 27602 G-6	TRADOC	Fort Eustis	SPPN	4Q18
372	FEUS_VA_TRA_03	U.S. Army Aviation Logistics School 27510 K-6	TRADOC	Fort Eustis	SPPN	4Q18
374	FEUS_VA_TRA_04	U.S. Army Aviation Logistics School 27510 G-2	TRADOC	Fort Eustis	SPPN	4Q18
376	FEUS_VA_TRA_06	U.S. Army Aviation Logistics School 27602 K-4	TRADOC	Fort Eustis	SPPN	4Q18
377	FEUS_VA_TRA_07	U.S Army Aviation Logistics School 27602 D-5	TRADOC	Fort Eustis	SPPN	4Q18
509	FEUS_VA_TRA_08	U.S Army Aviation Logistics School 27602 A5A	TRADOC	Fort Eustis	SPPN	4Q18
510	FEUS_VA_TRA_09	U.S Army Aviation Logistics School 27602 F10	TRADOC	Fort Eustis	SPPN	4Q18
511	FEUS_VA_TRA_10	U.S. Army Aviation Logistics School 27510 I-3	TRADOC	Fort Eustis	SPPN	4Q18
512	FEUS_VA_TRA_11	U.S. Army Aviation Logistics School 27510 A1B	TRADOC	Fort Eustis	SPPN	4Q18
513	FEUS_VA_TRA_12	U.S. Army Aviation Logistics School 2406 Room 1	TRADOC	Fort Eustis	SPPN	4Q18
514	FEUS_VA_TRA_13	U.S Army Aviation Logistics School 2411B Storage Room 1	TRADOC	Fort Eustis	SPPN	4Q18
515	FEUS_VA_TRA_14	U.S. Army Aviation Logistics School 2418 Room 27	TRADOC	Fort Eustis	SPPN	4Q18

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
972	FGRD_GA_TRA_06	SIGCoE LLC/TRADOC LLC Enterprise SIPR Facility	TRADOC	Fort Gordon	SPPN	4Q18
1120	JBLM_WA_TRA_01	JBLM_WA_Distance Learning 3201	TRADOC	Joint Base Lewis-McChord	SPPN	4Q18
1122	JBLM_WA_TRA_02	JBLM_WA_Distance Learning 6238	TRADOC	Joint Base Lewis-McChord	SPPN	4Q18
1380	FLEE_VA_TRA_05	FLEE CSSCLU 12420	TRADOC	Fort Lee	SPPN	4Q18
1558	POMR_CA_TRA_01	Naval Postgraduate School (NPS)	TRADOC	NAVSUPPDET Monterey CA	SPPN	4Q18
1587	FCBL_TN_TRA_01	FCBL Distributed Learning Center	TRADOC	Fort Campbell	SPPN	4Q18
201	FEUS_VA_TRA_01	Training Support Server Enterprise Center (TSSEC)	TRADOC	Fort Eustis	IPN	4Q22
3	FRKR_AL_TRA_01	DOSNET Data Center	TRADOC	Fort Rucker	SPPN	4Q24
75	FLVN_KS_TRA_01	BCBLL-BLCSE	TRADOC	Fort Leavenworth	SPPN	4Q24
79	FLVN_KS_TRA_04	TRAC-FLVN DC	TRADOC	Fort Leavenworth	SPPN	4Q24
110	FLWD_MO_TRA_01	Maneuver Support Battle Lab	TRADOC	Fort Leonard Wood	SPPN	4Q24
262	FGRD_GA_TRA_01	Experimentation Division (Battle Lab), Capabilities Development Integration Directorate (CDID)	TRADOC	Fort Gordon	SPPN	4Q24
267	FLEE_VA_TRA_03	SMARTNET - Simulation Training Center	TRADOC	Fort Lee	SPPN	4Q24
484	FLVN_KS_TRA_06	LD&E Data Center (BCNET)	TRADOC	Fort Leavenworth	SPPN	4Q24
616	FBNG_GA_TRA_02	McKenna Military Operations Urban Terrain Instrumentation Network	TRADOC	Fort Benning	SPPN	4Q24
619	FSIL_OK_TRA_04	Battle Lab (Building 3040)	TRADOC	Fort Sill	SPPN	4Q24
625	FSIL_OK_TRA_05	Mission Simulation Center (Building 3020)	TRADOC	Fort Sill	SPPN	4Q24
1144	FPLK_LA_TRA_01	FPLK_LA_MOUT 9951	TRADOC	Fort Polk	SPPN	4Q24
1274	FBNG_GA_TRA_06	Simulations Center FBNG 4105	TRADOC	Fort Benning	SPPN	4Q24
1276	FBNG_GA_TRA_07	Simulations Center FBNG 1J08	TRADOC	Fort Benning	SPPN	4Q24
1301	FJSN_SC_TRA_02	Soldier Support Institute Simulations Center	TRADOC	Fort Jackson	SPPN	4Q24

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
1364	FLVN_KS_TRA_11	FLVN NSC 45	TRADOC	Fort Leavenworth	SPPN	4Q24
1379	FLEE_VA_TRA_04	TRADOC-CASCOM-ADC001	TRADOC	Fort Lee	SPPN	4Q24
1507	FEUS_VA_TRA_16	LAB-ARCIC JAMSD BLCSE (ARCICBLCSE-FE)	TRADOC	Fort Eustis	SPPN	4Q24
1569	FHLT_CA_TRA_01	Virtual Simulation Center (VBS2)	TRADOC	Fort Hunter Liggett	SPPN	4Q24
1586	FCBL_KY_TRA_01	FCBL RVTT 3219	TRADOC	Fort Campbell	SPPN	4Q24
1588	FCBL_TN_TRA_01	Simulator for Raven UAVs	TRADOC	Fort Campbell	SPPN	4Q24
1589	FCBL_KY_TRA_13	Apache Simulator training	TRADOC	Fort Campbell	SPPN	4Q24
1590	FCBL_KY_TRA_14	Non-Rated Crew Member Manned Module	TRADOC	Fort Campbell	SPPN	4Q24
1591	FCBL_KY_TRA_03	Aviation Combined Arms Tactical Trainer	TRADOC	Fort Campbell	SPPN	4Q24
1592	FCBL_KY_TRA_04	Dismounted Soldier Training System	TRADOC	Fort Campbell	SPPN	4Q24
1594	FCBL_KY_TRA_06	Fort Campbell EST	TRADOC	Fort Campbell	SPPN	4Q24
1595	FCBL_KY_TRA_07	Route Clearance Operations	TRADOC	Fort Campbell	SPPN	4Q24
1596	FCBL_KY_TRA_08	Flight Simulator T-BOS for UH-60M	TRADOC	Fort Campbell	SPPN	4Q24
1597	FCBL_KY_TRA_09	Special Tasks Simulator	TRADOC	Fort Campbell	SPPN	4Q24
1598	FCBL_TN_TRA_02	Special Simulator - Aircraft Configuration Fidelity	TRADOC	Fort Campbell	SPPN	4Q24
1599	FCBL_KY_TRA_10	CFFT	TRADOC	Fort Campbell	SPPN	4Q24
1603	FCBL_KY_TRA_12	Coordinate Transportation Operations	TRADOC	Fort Campbell	SPPN	4Q24
COMMAND/PROPONENT: USACE						
986	FHAM_NY_ACE_01	CENAD Computer Room	USACE	USAG Fort Hamilton	IPN	1Q17
1225	FSFT_HI_ACE_01	Honolulu District Data Center	USACE	Fort Shafter	IPN	1Q17
604	CZMA_JP_ACE_01	JED Computer Room	USACE	Camp Zama	IPN	3Q17
597	ALXN_VA_ACE_01	HECSA/IWR Server Room	USACE	Fort Belvoir - Humphreys Engineer Center	IPN	4Q17
555	VCBG_MS_ACE_02	Vicksburg District Computer Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	3Q18

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
612	ALXN_VA_ACE_02	AGC Computer Room	USACE	Fort Belvoir - Humphreys Engineer Center	IPN	4Q18
1847	LTRK_AR_ACE_01	CESWL Data Center	USACE	Commercial Space - Leased Facility/Army Operated	SPPN	4Q18
1865	BAFB_CO_ACE_01	Buckley Resident Office Server	USACE	Buckley Air Force Base	IPN	4Q18
116	VCBG_MS_ACE_01	Central Processing Center	USACE	USACE/Engineer Research and Development Center	IPN	4Q21
546	CHCG_IL_ACE_01	CELRC LAN Room 606	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
547	WLMG_NC_ACE_01	CESAW Computer Room	USACE	U.S. Army Engineer District, Wilmington	IPN	4Q21
548	SVNH_GA_ACE_01	Savannah District Server Room	USACE	U.S. Army Engineer District, Savannah	IPN	4Q21
549	JCVL_FL_ACE_01	Jacksonville District Computer Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
550	MMPH_TN_ACE_01	Memphis District Computer Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
551	PHLA_PA_ACE_01	Philadelphia District Computer Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
552	CHTN_SC_ACE_01	Charleston District HQ - Hollings Hall	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
553	STLS_MO_ACE_01	St Louis District Computer Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
554	STPL_MN_ACE_01	Saint Paul District Data Center	USACE	U.S. Army Engineer District, St. Paul	IPN	4Q21

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
556	RCIS_IL_ACE_01	Rock Island District Computer Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
557	NWOR_LA_ACE_01	New Orleans District Server Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
559	CNCR_MA_ACE_01	New England Computer Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
561	TULS_OK_ACE_01	Tulsa District Computer Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
562	FTWO_TX_ACE_01	Fort Worth District Computer Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
563	LSAN_CA_ACE_01	Los Angeles Computer Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
564	PITB_PA_ACE_01	Pittsburgh District Data Center	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
565	CNCN_OH_ACE_01	CELRD Server Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
566	NSVL_TN_ACE_01	Nashville District Server Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
567	DTRT_MI_ACE_01	Detroit District Server Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
568	BFLO_NY_ACE_01	Buffalo District Computer Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
569	LSVL_KY_ACE_01	Louisville District Server Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
579	MOBL_AL_ACE_01	Mobile Information Technology Center	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
580	BLTM_MD_ACE_01	Baltimore Server Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
581	NRFL_VA_ACE_01	Norfolk Server Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
582	ELMN_AK_ACE_01	Alaska Server Room	USACE	Elmendorf AFB	IPN	4Q21
583	HNTN_WV_ACE_01	CELRH Basement Computer Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
587	SNFC_CA_ACE_01	San Francisco District Computer Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
588	SCRM_CA_ACE_01	Sacramento District Main Server Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
590	ALBQ_NM_ACE_01	CESPA Computer Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
591	KSCY_MO_ACE_01	CENWK Computer Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
592	STTL_WA_ACE_01	Seattle District Computer Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
594	OMAH_NE_ACE_01	Omaha District Computer Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
595	WLWL_WA_ACE_01	CENWW Computer Room	USACE	U.S. Army Engineer District, Walla Walla	IPN	4Q21
598	NYCX_NY_ACE_01	CENAN Computer/Server Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
599	HNVL_AL_ACE_01	CEHNC Computer Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
600	WASH_DC_ACE_01	HQUSACE Computer Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
601	ATLN_GA_ACE_01	SAD NOC	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
603	WNCH_VA_ACE_01	CEMED Computer Room	USACE	Commercial Space - Leased Facility/Army Operated	IPN	4Q21
606	YONG_KR_ACE_01	Fed Main	USACE	USAG Yongsan	IPN	4Q21
607	WBDN_DE_ACE_02	CENAU	USACE	USAG Wiesbaden	IPN	4Q21
608	KDHR_AF_ACE_01	CETAS Computer Room	USACE	Kandahar Airfield	IPN	4Q21
609	KBUL_AF_ACE_01	CETAN Computer Room	USACE	NEW KABUL COMPOUND	IPN	4Q21
988	NSMS_TN_ACE_01	USACE Finance Center Head End Room	USACE	Naval Support Activity Mid-South	IPN	4Q21
1931	GLTN_TX_ACE_01	Galveston District Data Center	USACE	U.S. Army Engineer District, Galveston, TX	IPN	4Q21
1964	HLBO_OR_ACE_01	Western Processing Center	USACE	Commercial Space - Outsourced	IPN	4Q21

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
COMMAND/PROPONENT: USACIDC						
1982	KSLT_DE_CID_01	5MP BN File Share and Print Server	USACIDC	USAG Kaiserslautern	SPPN	4Q16
928	FBLV_VA_CID_01	CITF	USACIDC	Fort Belvoir	IPN	4Q17
COMMAND/PROPONENT: USARC						
1397	FMCY_WI_ARC_01	FMCY ARC Pay 1951	USARC	Fort McCoy	IPN	4Q16
950	KSLT_DE_ARC_01	USAR 7th Civil Support Command Data Center	USARC	USAG Kaiserslautern	IPN	1Q17
275	FCRS_CO_ARC_01	COOP Data Center (Site Z)	USARC	Fort Carson	IPN	1Q18
388	FBRG_NC_ARC_01	Army Reserve Primary Data Center	USARC	Fort Bragg	IPN	3Q18
COMMAND/PROPONENT: USAREUR						
872	KSLT_DE_EUR_02	266th FMC	USAREUR	USAG Kaiserslautern	IPN	4Q16
574	GRAF_DE_EUR_03	JMTC TSAE STAMIS Applications	USAREUR	Grafenwoehr	IPN	3Q18
572	GRAF_DE_EUR_02	JMSC Camp Aachen	USAREUR	Grafenwoehr	IPN	4Q18
976	WBDN_DE_EUR_01	USAREUR ACA Test Lab	USAREUR	USAG Wiesbaden	SPPN	4Q18
977	KSLT_DE_EUR_03	USAREUR Miesau G4 STAMIS/LIS	USAREUR	USAG Kaiserslautern	SPPN	4Q18
1039	WBDN_DE_EUR_03	AFOD COMSOFT Building 1060	USAREUR	Clay Kaserne	IPN	4Q18
570	GRAF_DE_EUR_01	JMRC GTA Ranges Building 11840	USAREUR	Grafenwoehr	SPPN	4Q24
571	GRAF_DE_EUR_04	JMRC GTA Ranges Building 301	USAREUR	Grafenwoehr	SPPN	4Q24
573	GRAF_DE_EUR_05	JMRC HOHE - Main Post	USAREUR	USAG Hohenfels	SPPN	4Q24
COMMAND/PROPONENT: USASMDC/ARSTRAT						
6	RDST_AL_SMD_01	USASMDC-H Computer Room	USASMDC/ARSTRAT	Redstone Arsenal	IPN	4Q17
29	CLSP_CO_SMD_01	USASMDC-CS Computer Room	USASMDC/ARSTRAT	Peterson AFB	IPN	4Q18
722	HNVL_AL_SMD_01	Reagan Test Site Huntsville	USASMDC/ARSTRAT	Redstone Arsenal	IPN	4Q18
535	KWJA_MH_SMD_01	Reagan Test Site Kwajalein	USASMDC/ARSTRAT	U.S. Army Kwajalein Atoll	IPN	4Q21
COMMAND/PROPONENT: USMA						
143	USMA_NY_MAD_01	Washington Hall IPN	USMA	USMA West Point	IPN	4Q17

SEQ #	DATA CENTER ID	DATA CENTER NAME	ORGANIZATION	POST/CAMP/STATION	TYPE	QTR/FY
142	USMA_NY_MAD_02	Thayer Hall EDU SPPN	USMA	USMA West Point	SPPN	4Q18
144	USMA_NY_MAD_03	Mahan Hall EDU SPPN	USMA	USMA West Point	SPPN	4Q18
1156	USMA_NY_MAD_05	Jefferson Hall EDU SPPN	USMA	USMA West Point	SPPN	4Q18
1170	USMA_NY_MAD_06	Washington Hall EDU SPPN	USMA	USMA West Point	SPPN	4Q18
1175	USMA_NY_MAD_07	USMAPS EDU SPPN	USMA	USMA West Point	SPPN	4Q18
1178	USMA_NY_MAD_10	Lincoln Hall EDU SPPN	USMA	USMA West Point	SPPN	4Q18
OTHER						
Command: JSP Transfer (* Once transfer is complete, no longer tracked in Army Inventory)						
949	ARTN_VA_OAA_01	Taylor Building Lab	OAA	Commercial Space - Leased Facility/Army Operated	SPPN	4Q18
210	PENT_DC_OAA_01	USAITA Pentagon Data Center	OAA	Pentagon	IPN	4Q19
1412	ALXN_VA_OAA_02	Mark Center Data Center	OAA	Pentagon	IPN	4Q21

ARMY SYSTEMS AND APPLICATIONS EXCLUDED FROM MIGRATION

1. These categories of systems and applications are excluded from migration to approved enterprise hosting environments.

a. Systems designated as critical military intelligence or cryptologic 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 in reference l.

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

c. Training simulators and simulations, weapons system specific and non-systems training aids, devices, simulators, and simulations. This exclusion does not include mission training centers and mission training simulation centers.

d. Industrial control systems and supervisory control and data acquisition systems that support Army missions, as defined in National Institute of Standards and Technology (NIST) Special Publication 800-82 in reference m. Both types of systems, which support Army missions, include a variety of systems and mechanisms used to monitor and/or operate critical infrastructure elements that require onsite presence, such as electricity, water, natural gas, fuels, entry and access, heating and air-conditioning, runway lighting, and so on.

e. U.S. Army Medical Command will continue to follow Military Health Systems procedures; its enterprise applications are excluded from this policy.

f. Existing Defense Research Engineering Network (DREN) applications and systems have unique requirements that may render migration to enterprise hosting environments detrimental to the mission and operations they support. Army commands may request a DREN application migration waiver from the Migration Implementation and Review Council.

(1) Army commands that choose to migrate DREN applications to an enterprise hosting environment will follow established processes for application migration, including collaborating with the Army Application Migration Business Office; completing rationalization, review, and endorsement through the appropriate domain and mission area governance forums; and completing a cost-benefit analysis (if required by reference f).

(2) Before beginning development, new applications and systems with specific mission and operational requirements that restrict hosting options to the DREN must submit a disposition waiver through their organizational channels for endorsement by

the senior general officer or member of the Senior Executive Service and submission to the Army Chief Information Officer/G-6 for review and approval.

(3) Migration of applications and systems from other DoD networks to the DREN for the sole purpose of avoiding migration to an enterprise hosting environment is prohibited.

g. All U.S. Army Special Operations Command data centers and applications will comply with data center closure requirements directed by U.S. Special Operations Command.

2. Enterprise Resource Planning Systems (ERPs). The Army must migrate major ERP and key ERP-enabling systems to a Defense Information Systems Agency Defense Enterprise Computing Center by the end of FY 18. These systems include but are not limited to:

a. General Fund Enterprise Business System / General Fund Enterprise Business System – Sensitive Activities.

b. Global Combat Support System - Army.

c. Logistics Modernization Program.

d. Integrated Personnel and Pay System - Army.

e. Army Enterprise Systems Integration Program.

f. Logistics Information Warehouse.

GLOSSARY OF APPLICATION MIGRATION TERMS

Term	Definition	Source
Application	Software that performs a specific task or function, such as word processing, creating spreadsheets, generating graphics, or sending email. For purposes of reporting in the Army Portfolio Management Solution (APMS), applications may be listed as a separate investment or included in an information system registration. If reported as a separate investment, the application will identify in the dependency tab the host system it resides on as the parent information system.	Army Regulation (AR) 25-1, 25 June 2013 (reference p)
Application or System Owner	The system proponent and the agency or organization that establishes the need for the information technology (IT) system. Develops requirements, provides funding, designates who will manage data entry, and aligns requirements with APMS standards.	AR 25-1, 25 June 2013 (reference p)
Army Application Migration Business Office (AAMBO)	The Program Executive Office Enterprise Information Systems, in coordination with the Army Chief Information Officer (CIO)/G-6, established AAMBO, as directed by reference a, to serve as the Army's single point of contact for system and application owners. AAMBO provides assistance in defining requirements, recommending the most cost-effective hosting solution, and supporting system and application owners throughout the application migration process.	Under Secretary of the Army (USA) Application Migration Policy Memorandum, 9 June 2014, (reference a)
Cloud Access Point	A Department of Defense (DoD) cloud access point is a system of network boundary protection and monitoring devices, otherwise known as an information assurance stack, through which cloud service provider infrastructure will connect to a DoD Information Network (DoDIN) service, the Non-Secure Internet Protocol Router Network (NIPRNet) or the Secret Internet Protocol Router Network (SIPRNet).	DoD Cloud Computing Security Requirements Guide (reference h)
Cloud Computing	A model for enabling on-demand network access to a shared pool of configurable IT capabilities and resources (such as networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports the services. True cloud computing includes five essential characteristics: on-demand self-service, ubiquitous network access, location-independent resource pooling, rapid elasticity, and measured service. It has three service delivery models (software as a service, platform as a service, and infrastructure as a service) and four enterprise access models (Private, Community, Public, and Hybrid clouds).	National Institute of Standards and Technology Special Publication (NIST SP) 800-145 (reference t)
Cloud Service Provider/Cloud Service Offering	A cloud service provider is an organization that provides cloud services. These services come in a variety of service and deployment models, but their characteristics involve one or more of the following: on-demand self-service, resource pooling, rapid elasticity, measured service, and broad network access. The cloud service offering is a specific set of services the cloud service provider makes available to cloud consumers.	NIST SP 800-145 (reference t) and NIST SP 800-146 (reference v)

Term	Definition	Source
Core Data Center	The backbone of the Joint Information Environment (JIE), core data centers (CDCs) are highly capable, highly resilient data centers that provide standardized hosting and storage services to the enterprise within the single security architecture now being implemented, as described in reference e. CDCs also enable a significant reduction in the total number of DoD data centers by serving as consolidation points for computing and storage services currently hosted across hundreds of component facilities.	DoD CIO JIE Memorandum, 11 July 2013 (reference e)
Computer Network Defense Service Provider	The responsibilities of the computer network defense service provider include incident, event, and problem management, in accordance with DoD Directive 8530.01. Second Army, in coordination with U.S. Army Cyber Command, is designated as the Army's computer network defense service provider in accordance with reference p.	AR 25-1, 25 June 2013 (reference p)
Enterprise Data	Data shared across systems, applications, and processes by organizations, branches, divisions, and other subunits in the enterprise.	AR 25-1, 25 June 2013 (reference p)
Enterprise System	An application that passes data across an installation boundary.	CIO/G-6 ITAS/Goal 1 Waiver Memorandum (reference k)
Geographically Separated Unit	A facility that is connected to a CDC or installation processing node (IPN) via a dedicated fiber connection or point-to-point circuit. No JIE single security architecture devices or hosting of applications or systems is available at the unit.	DoD CIO Joint Information Environment Memorandum, 11 July 2013 (reference e)
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 (for example, cloud bursting for load balancing between clouds).	NIST SP 800-145 (reference t)
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For the purposes of this definition, equipment is used by an executive agency if the executive agency directly uses the equipment or a contractor is under a contract with the executive agency that (i) requires the use of such equipment or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the provision of a product. The term "IT" includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.	40 U.S.C. § 11101 (adapted) 40 U.S.C. § 1401 (adapted) Committee on National Security Systems Instruction 4009 (reference y)
Information System	The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. For the purposes of APMS, the terms "application" and "information system" are both IT	AR 25-1, 25 June 2013 (reference p)

Term	Definition	Source
	investments describing a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information). The application of IT to solve a business or operational (tactical) problem creates an information system.	
Infrastructure as a Service	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 underlying cloud infrastructure, but has control over operating systems, storage, and deployed applications and possibly limited control over select networking components (for example, host firewalls).	NIST SP 800-145 (reference t)
Installation Processing Node	A fixed DoD data center serving a single DoD installation and local area (installations physically or logically behind the network boundary) with local services that cannot (technically or economically) be provided from a CDC. A DoD installation will have no more than one IPN but each node may have multiple enclaves to accommodate unique installation needs (such as Joint bases).	DoD CIO JIE Memorandum, 11 July 2013 (reference e)
Installation Services Node	A facility containing the localized equipment necessary to provide the minimum basic functionality to an installation should it become disconnected from the DoDIN (formerly the Global Information Grid). No application hosting or data processing occurs in an installation service node. Potential services include read-only Active Directory servers, Domain Name System servers, Assured Compliance Assessment Solution servers, Host-Based Security System servers, and print servers. In addition, the nodes may host the elements of unified capabilities that must remain on the installation to enable emergency services even when the connection to the DoDIN is interrupted.	DoD CIO JIE Memorandum, 11 July 2013 (reference e)
Joint Information Environment	A secure environment composed of shared IT infrastructure, enterprise services, and a single security architecture designed to achieve full-spectrum superiority, improve mission effectiveness, increase security, and realize IT efficiencies. The JIE is operated and managed in accordance with the Unified Command Plan, using enforceable standards and specifications, and common tactics, techniques, and procedures.	DoD Instruction 8320-02P, 5 August 2013 (reference o)
Kill	The application is not necessary and the application will be terminated.	USA Application Migration Policy Memorandum (reference a)
Migrate	Move applications and systems from the current hosting facility to a DoD- or Army-approved hosting environment.	USA Application Migration Policy Memorandum (reference a)
Mission Command	Mission command is the exercise of authority and direction by the commander, using mission orders to enable disciplined initiative within the commander's intent to empower agile and adaptive leaders in the conduct of unified land operations. Mission command systems include personnel, networks, information	Army Doctrine Publication 6-0 (reference u)

Term	Definition	Source
	systems, processes and procedures, facilities, and equipment that enable commanders to conduct operations.	
Modernize	Applications that are useful and needed throughout the Army (beyond fiscal year 2018) should be "modernized." Modernized applications should be updated to Army Data Center Computing Environment standards and an expected modernization date should be assigned.	USA Application Migration Policy Memorandum (reference a)
National Security Systems	Any telecommunications or information system the U.S. Government operates, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or matters critical to the direct fulfillment of military or intelligence missions.	AR 25-1, 25 June 2013 (reference p)
Platform as a Service	The capability provided to the consumer is to deploy onto cloud infrastructure consumer-created or acquired applications that were developed by using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure, including the network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application hosting environment.	NIST SP 800-145 (reference t)
Personally Identifiable Information/ Privacy Data	Information that can be used to distinguish or trace an individual's identity (for example, name, Social Security number, and biometric records) or, when combined with other personal or identifying information, is linked or linkable to a specific individual (for example, date and place of birth, mother's maiden name).	AR 25-1, 25 June 2013 (reference p)
Rationalization	Portfolio rationalization, or portfolio management, is the systematic management of IT investments within a portfolio, which includes identifying, prioritizing, authorizing, managing, and controlling applications. Managing these investments across Army commands, domains, mission areas, and the enterprise will help the Army to effectively support its military objectives while reducing costs. Army portfolio management is a multitiered approach that seeks to categorize, evaluate, and manage the universe of software applications that support Army missions worldwide. It divides the task into Army organizational level, domain level, mission area level, and enterprise level, delegating the responsibility for evaluation to those commanders closest to the mission being supported.	USA Application Migration Policy Memorandum (reference a)
Software as a Service	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 either a thin-client interface, such as a Web browser (such as Web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure, including the network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited configuration settings for user-specific applications.	NIST SP 800-145 (reference t)

Term	Definition	Source
Special Purpose Processing Node	A fixed data center supporting special purpose functions that cannot (technically or economically) be supported by CDCs or IPNs because of association with infrastructure or equipment (for example, communications and networking, manufacturing, training, education, meteorology, medical, modeling and simulation, and test ranges). No general-purpose processing or storage can be provided by or through a special purpose processing node. They do not have a direct connection to the DoDIN and must connect through a CDC or IPN.	DoD CIO JIE Memorandum 11 July 2013 (reference e)
Sustain	The ability to maintain the level and duration of operational activity necessary to achieve military objectives. Applications that do not meet the definitions of "kill" or "modernize" will be classified as "sustain." The application is necessary but cannot be upgraded. The application will need to be migrated to an enterprise hosting facility, but may require a waiver if it does not conform to JIE or Common Operating Environment standards.	USA Application Migration Policy Memorandum (reference a)
Tactical Processing Node	Tactical or mobile processing nodes will provide services similar to a CDC but are optimized for the tactical or deployed environment. Depending on the circumstances, the nodes may connect to the DoDIN though DoD satellite gateways.	DoD CIO JIE Memorandum 11 July 2013 (reference e)
Virtualization	The act of creating a virtual (instead of an actual) version of something, including but not limited to, a virtual computer hardware platform, operating system, storage device, or computer network resources.	USA Application Migration Policy Memo (reference a)