

USAREC Regulation 25-1

Information Management

**Information
Resource
Management
Program**

**Headquarters
United States Army Recruiting Command
Fort Knox, Kentucky
27 March 2019**

UNCLASSIFIED

SUMMARY of CHANGE

USAREC Reg 25-1

This expedited revision dated 27 March 2019 supersedes UR 25-1 dated 14 November 2018.

- o Makes administrative changes (throughout) for page number changes.
- o Adds the USAREC Form 25-1.2 (Communications Relocation Checklist) as Figure 2.2
- o Adds 2-6 b. (4)

Information Management
Information Resources Management Program

For the Commander:

WAYNE R. HERTEL
Colonel, GS
Chief of Staff

Official:

Ronnie L. Creech
Ronnie L. Creech
Assistant Chief of Staff, CIO/G-6

History. This expedited revision supersedes the UR 25-1 dated 14 November 2018. The effective date is 27 March 2019.

Summary. This regulation establishes policy and assigns responsibilities for governance of information management (IM) and information technology (IT) for U.S. Army Recruiting Command (USAREC) organizations. IM/IT addresses the management of information as a resource, the technology supporting information requirements, and knowledge management enablers as a means to achieve a net-centric knowledge-based force. The scope of Chief Information Officer (CIO) responsibilities and management processes is delineated throughout this regulation IAW AR 25-1.

Applicability. This regulation applies to all USAREC activities, portions of this regulation prescribe specific prohibitions that are punitive, and violations of these provisions may subject offenders to non-judicial or judicial action under the Uniform Code of Military Justice.

Proponent and exception authority. The proponent of this regulation is the Chief Information Officer/G-6. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of LTC or the civilian equivalent of GS14.

Army management control process. This regulation contains management control provisions in accordance with AR 11-2 but does not identify key management controls that must be evaluated.

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from

the USAREC Chief Information Officer/G-6 (RCIO), 1307 3rd Ave., Fort Knox, KY 40121.

Relationship to USAREC Reg 10-1.

This publication establishes policies and procedures regarding Information Technology according to UR 10-1 para 3-16 b.

Suggested improvements.

The proponent agency of this regulation is the Office of the Director of Information Management. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQ USAREC (RCIO-OPP), Fort Knox, KY 40121-2726.

Distribution. Distribution of this regulation has been made in accordance with USAREC Pam 25-30, distribution B. This regulation is published in the Recruiting Company Operations and Administration UPDATE.

*This regulation supersedes USAREC Regulation 25-1(V2), dated 14 November 2018.

Contents (Listed by paragraph and page number)

Chapter 1

Introduction, page 1

Purpose • 1-1, *page 1*

Scope • 1-2, *page 1*

References • 1-3, *page 1*

Explanation of abbreviations and terms • 1-4, *page 1*

Responsibilities • 1-5, *page 1*

Other Army Organizations • 1-6, *page 2*

Chapter 2

Governance, page 3

General • 2-1, *page 3*

Governance Structure • 2-2, *page 3*

Governance Process • 2-3, *page 3*

Decision Baselines • 2-4, *page 4*

Enterprise Solutions • 2-5, *page 4*

Reporting Requirements • 2-6, *page 4*

Strategic Planning • 2-7, *page 6*

IT Asset Management Program • 2-8, *page 8*

Chapter 3

Capital Planning and Investment Management, page 8

Portfolio Management Overview • 3-1, *page 8* Developing a
Business Case • 3-2, *page 8*

Milestone Reviews • 3-3, *page 8*

Submitting Capability Requests • 3-4, *page 8*

Resource Management • 3-5, *page 8*

Types of Funds • 3-6, *page 9*

Validated UFRs • 3-7, *page 9*

IM/IT and Telecommunications Acquisitions • 3-8, *page 9*

Contracts • 3-9, *page 10*

Chapter 4

Knowledge Environment, page 11

General • 4-1, *page 11*

Collaboration Capabilities • 4-2, *page 11*

Content Management • 4-3, *page 11*

Records Management • 4-4, *page 13*
Portal/Web Site Administration • 4-5, *page 13*

Chapter 5

Network Operations, *page 15*
RSN-Provided Infrastructure • 5-1, *page 15*
Mission Support • 5-2, *page 15*
Network Access • 5-3, *page 15*
Wireless Networks • 5-4, *page 15*
Appropriate Use of Communications Systems • 5-5, *page 16*
Command, Control, Communications & Computers (C4) Reporting • 5-6, *page 16*

Chapter 6

Cybersecurity, *page 16*

Appendix A.

References, *page 17*

Appendix B.

Metadata and Taxonomies, *page 18*

Table List

USAREC Records Management Duties and Responsibilities • Table 4- 1, *page 14*

Figure List

Validation of Phone bills • Figure 2- 1, *page 6*
Communications Relocation Checklist • Figure 2- 2, *page 7*

Glossary

This page left intentionally blank.

Chapter 1 Introduction

1-1. Purpose.

USAREC is the creator and owner of much of the Army's authoritative information, e.g., personal information, background and enlistment eligibility, accessioning, and creation of official Soldier records. USAREC is the proponent and authoritative data source for specific categories and subjects of Army information. Information fuels our ability to effectively execute our missions and functions for the Army and enables command and control in the organization. Information requires management, enabling resources (hardware, software, skilled personnel), and processes to assure its availability and effective use.

1-2. Scope.

This regulation establishes policy for Information Management (IM), the supporting of Information Technology (IT), and the enablers to Knowledge Management (KM) in USAREC. IT includes any information system, component, equipment, services, collection of hardware and software, or similar products that USAREC uses to access, collect, process, store, transmit, display, and disseminate information. IM is the planning, budgeting, manipulating, and controlling of information throughout its lifecycle. KM enablers are the technologies and processes that support access to and exchange of relevant information.

1-3. References.

Appendix A contains the required and related publications.

1-4. Explanation of abbreviations and terms.

The glossary contains abbreviations and special terms used in this regulation.

1-5. Responsibilities.

a. The USAREC CIO will—

(1) Establish policy for the management of information resources and the programming, funding, and acquisition of IM/IT assets and services.

(2) Develop guidance and plans for managing IM/IT investment strategies. Advise the USAREC leadership and staff in the prioritization of IM/IT requirements for funding.

(3) Assist the Deputy Chief of Staff G-4/8 in determination of appropriate use of Operation and Maintenance, Army (OMA and Other Procurement, Army (OPA) funding for IM/IT acquisitions. Review all spending plans with an IM/IT component before submission and execution.

(4) Manage the process for IM/IT acquisitions that require Headquarters (HQ) USAREC approval to include requirements that will incur a recurring obligation, for example, long haul communications services, desktop video teleconferencing, monthly/yearly user fees, etc.

(5) Chair the USAREC Information Technology Steering Committee (ITSC). Provide guidance to all.

(6) Manage the Command Cyber Security Program, per Army Regulation (AR) 25-2 and USAREC Pam 25-1-1.

(7) Provide the Command Publications and Records Manager.

(8) Serve as the principal staff officer for IM/IT matters to the Commanding General, advising in all matters related to IT.

(9) Establish IT Asset Management program for the systematic identification, acquisition, utilization, sustainment, retirement and removal of IT assets in the USAREC inventory.

b. The HQ USAREC Deputy Chief of Staff G3 will incorporate IM/IT processes and requirements outlined in this regulation into the development of training, education, and leader development strategies and programs.

c. The HQ USAREC G4/8 will:

(1) Centrally manage USAREC's Planning, Programming, Budgeting, and Execution System (PPBES) activities to include procedures to obtain funds for IM/IT.

(2) Coordinate OMA/OPA with CIO prior to decision.

(3) Coordinate management decision documents for all service contracts with an IM/IT component with the USAREC CIO.

(4) Coordinate funding requests for projects that include IM/IT with USAREC CIO for technical review and approval.

d. Headquarters USAREC Public Affairs Officer (PAO) will—

(1) Coordinate the USAREC corporate information content and major themes on the USAREC public homepage and

pages linked off the USAREC homepage.

(2) Serve as USAREC web content manager for the USAREC public web site.

(3) Review materials prior to posting on a public web site. Ensure content provider has coordinated with local operations security (OPSEC) officer and SJA for review prior to releasing information.

(4) Coordinate with the USAREC CIO on any content that may affect the supporting IT or conformance with policies related to IT.

e. USAREC G2 will –

(1) Serve as proponent for the policies and procedures used by USAREC organizations to acquire models and simulation systems.

(2) Coordinate with USAREC CIO for architectural integration of those systems during requirements development.

f. USAREC Commanders, Commandants, and Directors will —

(1) Establish processes and programs to effectively manage their information resources.

(2) Assign responsibilities to execute Army and USAREC IM/IT policies and coordinate the management and operation of IM/IT to support mission requirements. This regulation refers to those individual(s) assigned to the S-6 staff with a USAREC Brigade or Battalion. Staff S-6 responsibilities are detailed in USAREC Pamphlet (PAM) 25-1-1.

(3) Maintain accurate information on their IM/IT assets in the use of network readiness, investment management, and architecture development decisions.

(4) Prepare documentation regarding IM/IT acquisitions and comply with reporting requirements as stated throughout this regulation. Submit documentation to USAREC CIO for acquisitions outside local approval authority.

(5) Obtain approval of IA certification, accreditation, and net-worthiness documentation prior to systems implementation.

(6) Coordinate with USAREC CIO prior to acquisition of any IM/IT that will be connected to the installation local or wide area networks.

(7) Establish procedures and assign responsibilities to manage the information/content life cycle in repositories, databases, portals, web sites, and shared drives.

(a) Assign responsibilities for the management and administration of command/activity public web sites.

(b) Assign an administrator to manage all user accounts associated with information systems/capabilities.

(8) Establish procedures and assign responsibility for records management IAW AR 25-400-2.

(9) Ensure Information Assurance Vulnerability Management (IAVM) compliance language is included in pertinent contracts and acquisitions. The IT service provider operates the Integrated Automaton Architecture (IAA) in support of the U.S. Army Recruiting Command and U.S. Army Cadet Command and provides network support for U.S. MEPCOM and other Human Resources Command (HRC) mission areas. DA recognizes HRC PERSINSD role as the single, centralized authority responsible for operating the enterprise-wide IAA. This authority is under the technical direction of IT service provider and the established procedures for the DA Human Resources Domain. HRC responsibility includes IAA operations, maintenance, sustainment, evolution, business decisions, and acquisition strategies. USAREC authorizes IT service provider to operate and maintain the AAC-IAA within existing Federal, Department of Defense (DOD), and DA guidance.

g. Staff Judge Advocate (SJA) at HQ and activity level will review materials, per requests from commands, units, or organizations, prior to posting on a public web site.

h. PAO at activity level will

(1) Review materials prior to posting on a public web site. Ensure content provider has coordinated with local operations security (OPSEC) officer and SJA for review prior to releasing information.

(2) Serve as web site content manager for the activity's public web site.

(3) Establish local procedures, in coordination with the local OPSEC officer, SJA, Assistant Chief of Staff G7/9, for review and clearance of information posted to the assigned USAREC organization's web sites.

(4) Coordinate incorporation of USAREC and local strategic communications themes into public web sites.

1-6. Other Army Organizations.

USAREC organizations will comply with policies, procedures, and standards established by the following organizations:

a. The Army CIO/G6 has statutory authority for the effective and efficient use of IT in the Army and exercises oversight for all IM/IT expenditures and investments. CIO/G6 approves the release of all OPA funds for IM/IT investments and the use of OMA funds for IM/IT acquisitions over the DA-determined threshold when funds are not allocated specifically for IT.

b. IT service providers provides strategic plans, standards, and technical guidance for the Recruiting Services Network (RSN) and all IM/IT managed at the enterprise level. IT service providers executes technical control over all enterprise systems and applications.

c. IT Service providers provide architectural authentication and validation of IM/IT equipment or services connected to USAREC authorized networks operating in the military and commercial environments. The IT service providers provide USAREC organizations common-user baseline services as specified in the Command, Control, Communications, and Computer Information Management Services List and support as identified in specific service level agreements and memorandums of agreement.

d. The Army Contracting Command (ACC) provides contracting policy and support to all Army organizations through installation Mission Installation Contracting Command offices.

e. The Program Executive Office-Enterprise Information Systems negotiates and manages enterprise IM/IT contracts for hardware, software, and services.

f. DA-G2. Provides security guidance concerning content classification.

Chapter 2 Governance.

2-1. General.

Planning for the effective and efficient use of IM/IT within USAREC is not a “govern-once” activity that happens at the end of the fiscal year. Full cycle governance is an overall deliberate planning process that links sound IM/IT investments to enhanced mission planning and execution. Governance provides visibility of IM/IT spending and maintains focus on those activities that have the most strategic value to the command. IM/IT governance is an ongoing process of selecting, controlling, and evaluating solutions and starts with the identification of a functional need or requirement solution that can be enabled by use of IT.

2-2. Governance Structure.

The USAREC governance structure consists of the ITSC and CIO subject matter experts (SME).

a. The CIO is responsible for recommending enterprise requirements and investments to the USAREC Deputy Commanding General (DCG). The CIO reviews the business case for IM/IT investments to assess that the IM/IT initiative is aligned with USAREC and Army strategic goals, supports maximum efficiency of USAREC spending, and makes considered decisions about where IM/IT resources should be focused based on project/system risks, impacts, performance, and documented best business practices. IM/IT initiatives will be reviewed by the CIO via an electronic collaborative staffing process. The CIO, G-6 SME and ITSC members will discuss strategic direction for IM/IT in the command, prioritize unfunded IT requirements, and perform milestone reviews of existing investments.

b. The CIO reviews and prioritizes initiatives and requests for new capabilities and upgrade/modernization requirements for IT that must satisfy USAREC-wide requirements, affects military and USAREC authorized networks operating in the military and commercial environments across or beyond USAREC, or impacts existing Service Level Agreements in USAREC. The CIO looks at any requirement having these characteristics, regardless of anticipated cost. Decisions and recommendations made by the CIO may impact all USAREC organizations. The CIO reviews requirements and IM/IT solutions for policy and standards compliance, technical feasibility and integration, scope, cost, and impact on the network and architecture.

2-3. Governance Process.

a. Requirements Submission. Sponsors submit their workplace and mission unique IM/IT requirements with the Information Technology Equipment Procurement & Service (ITEPS System) through their S-6 to the CIO. BDE S-6 will validate the requirement to ensure it meets organizational goals and forwards to the USAREC CIO. The ITEPS form is a fillable template located on the S6 Zone at <http://span.usarec.army.mil/sites/HQ/G6/SitePages/S6Z-RequestCenter.aspx>.

b. CIO Review. CIO will contact the submitter of the requirement, as necessary, and meet to discuss ongoing issues concerning submitted requirements. The CIO validates and/or determines the best technical solutions for requirements or, based on the scope and/or cost of the requirement, will approve, disapprove, or make a recommendation to the CIO. The CIO goal for disposition of requests is 5 days. However, requirements with a high dollar value or requirements that require more detailed evaluations, assessments, or testing by technical SME, may not meet the preferred 5-day disposition window.

c. Disapproval. If the requirement is disapproved, the submitting organization will be notified by the CIO via e-mail, within 2 working days of disapproval. The e-mail will contain information explaining the reason(s) for the disapproval. A requirement below the regulated threshold can be disapproved at any level of the governance structure. Submitting organizations can appeal by sending an e-mail to the CIO/G-6 or S-6 and updating the ITEPS form with additional information to address concerns of the governance entities that reviewed and denied the request. The BDE S6 may coordinate with the USAREC CIO to reevaluate the request.

d. Conflict Resolution. The USAREC CIO will be the primary conflict resolution entity within the defined IM/IT

governance structure. The CIO will make the final decision on a below-threshold request. If an organization is not satisfied with the decision or results of the appeal, the issue may be resubmitted via the process described in para c. above.

2-4. Decision Baselines.

USAREC organizations will consider the following criteria when developing or assessing IM/IT solutions:

- a. Security is a high priority and may be a more critical attribute than ease of use, accessibility, etc. when it comes to IM/IT use and purchase in USAREC. Information systems must meet the approved DOD and DA security requirements as stated in AR 25-2.
- b. Use of mandatory contracts and Army command license availability where applicable.
- c. Expected benefit or other impact to functional processes and consistency with CG, USAREC priorities, e.g., as documented in USAREC Campaign Plan, USAREC Budget Guidance, Information Management Strategic Plan, and other documents.
- d. Risk (e.g., technical difficulty to implement, user acceptance, immediacy and longevity of the benefits, compatibility with existing organizations and personnel skills.)
- e. Compatibility with other planned or fielded IM capabilities in the command and on the installation.
- f. Existence of like requirements and utility of a solution as a pilot for the initiation of a command-wide program.
- g. Applicability of the solution for fielding beyond the target functional area (i.e., horizontal technology integration).
- h. Compatibility with DOD or Army managed programs.
- i. Consistency with standards in the Defense Information Standards Registry and the architectural guidance as published by the USAREC CIO.
- j. Return on investment and use of the appropriate category of funds (OMA and OPA). Planning for and ability to sustain the system.
- k. Ability to secure the information to be processed and stored.

2-5. Enterprise Solutions.

USAREC will capitalize on enterprise solutions, consolidated buys, and low cost/no cost solutions such as AKO to infuse our business processes with knowledge-based qualities, such as improved access to information and collaboration.

- a. When applicable, capabilities will be optimized for the command vice the local level. Requirements common to multiple USAREC organizations are best supported with a common enterprise solution that promotes standardization and a consolidated execution plan that promotes efficiency.
- b. Standardized solutions for similar requirements are preferable over equal or slightly more capable unique solutions.
- c. USAREC relies on the IT Service Provider for infrastructure support and favors solutions that are Service provider delivered and meet the minimum standard for mission execution.
- d. USAREC will use enterprise software agreements and hardware and services contracts managed by the Army Computer Hardware Enterprise Software and Solution (CHESS) as its first source for IM/IT acquisitions for workplace and appropriate mission systems.
- e. The Army Consolidated Buy (CB) Program consolidates Army requirements for desktops and laptops to get the best price for the enterprise and will be utilized by the USAREC G6. Instructions for the CB, product descriptions, and detailed ordering procedures are posted on CHESS web site <https://chess.army.mil/>.

2-6. Reporting Requirements.

Proponents of IM/IT based systems have various reporting requirements for DOD, Army, and USAREC.

- a. ITASS (formerly Goal 1). USAREC G6 must obtain a waiver from HQDA CIO/G6 to use non-IT programmed funds for the purchase of all IM/IT goods and services over \$25K OMA and \$100K Research, Development, and Acquisition. Thresholds are cumulative and IM/IT expenditures include all hardware, software, development, services, contractor support, testing, licenses and maintenance fees, web site and portal expenses, audio visual, and communications capabilities.
- b. Army Portfolio Management Solution (APMS) – Army Information Technology Repository (AITR). The AITR is the Army's single, authoritative registry for IM/IT systems and is a module in the APMS. IM/IT systems must be entered in APMS-AITR if they meet criteria published in the Army Knowledge Management Guidance Memorandum - Capabilities-Based IT Portfolio Governance Implementing Guidance posted on the IT RAD portal. USAREC system proponents enter system data and congressionally mandated reporting requirements through APMS-AITR:

(1) Federal Information Security Management Act (FISMA) mandates that the security status of Army information systems be documented, updated, and verified at least annually. Security requirements are specified in AR 25-2. System proponents will use AITR to report FISMA compliance. FISMA guidance and mandates are posted on the IT RAD portal

on AKO.

(2) Business Management Modernization Program (BMMP). DOD requires certification of defense business systems costing over \$1M. If a system requires \$1M or more in modernization costs, the Army Domain Lead may require additional data in APMS. To determine the systems that meet the criteria for reporting go to http://www.dod.mil/bmmp/faq_certification.html.

(3) Certification of commercial telephone bills assigned to your unit/activity must be documented on USAREC Form 25-1.1 (Validation of Phone bills), and returned to the Network Enterprise Center (NEC) Telephone Service Section (TSS) and the USAREC CIO immediately. All billing discrepancies and charge disputes should be reported to the NEC TSS and the USAREC CIO immediately. The Telephone Control Officer (TCO) signature concurs adherence with AR 25-13 and all toll charges or calls not determined official or not in the best interest of the U.S. Government must be listed in an attachment to the UF 25-1.1 (Validation of Phone bills).

(4) During PAE or planned station/company/battalion and brigade moves, when the unit has a signed lease, the S-6 will initiate and use the USAREC Form 25-1.2 (Communication Relocation Checklist). Telephone installation can take up to 60 days and Network installation could take up to 120 days. This time starts when USAREC receives the request for service (RFS). Attach the UF 25-1.2 to the RFS when sending it to USAREC G-6 operations at the following link: <https://span.usarec.army.mil/sites/HQ/G6/Lists/TelecomRequest>.

Figure 2-1 Validation of Telephone bills


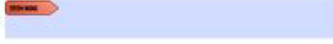
VALIDATION OF TELEPHONE BILLS	
PART I - TYPE OF BILL	
<input type="checkbox"/> Commerical Calls	<input type="checkbox"/> DSN Calls
PART II - USER'S INFORMATION	
SUSPENSE	<input type="text"/>
NAME OF USER / UNIT	<input type="text"/>
TELEPHONE NUMBERS	<input type="text"/>
BILLING PERIOD	<input type="text"/> THROUGH <input type="text"/>
PART III - BDE VALIDATORS RESPONSIBILITY	
<p>Attached is the invoice of charges for the commercial telecommunication services provided to your unit/agency. If an account or number enclosed is not assigned to you or your unit/activity, please annotate this fact on the statement and return it to the USAREC Governance Division immediately. If any billing discrepancy or charge dispute exist please report it to the USAREC Governance Division immediately. Each detailed billing statement reflects services toll charges, basic fees accrued during the above billing period and will be charged to your unit/agency account.</p> <p>As the Brigade Validation Authority, you must validate that all incurred charges in the attached billing statement(s) were authorized and/or necessary for the performance of official government business, as required in AR 25-13. All charges or calls determined not to be official and in the best interest of the U.S. Government must be listed in an attachment to the basic correspondence. Please indicate the user's telephone number, telephone call(s), and action(s) taken to recover money due to the U.S. Government. Refer to DA Pamphlet 25-1-1 for specific courses of action.</p> <p>Please digitally sign and return this certification to USAREC Governance Division via e-mail at usarmy.knox.usarec.mesg.hq-g6-governance@mail.mil Failure to complete and return this certification in a timely manner may result in termination of this commercial service.</p>	
DATE	BDE VALIDATOR'S SIGNATURE 
PART IV - CERTIFICATION OF BILLS	
I certify that (please check the appropriate line item)	
<input type="checkbox"/> All calls in this usage report were made in the conduct of Official Business within AR 25-13.	
<input type="checkbox"/> Checked or highlighted charges in the attached were found not to be official government business and were unauthorized.	
<input type="checkbox"/> The statement(s)/ telephone number(s) in this enclosed is (are) not under my responsibility.	
DATE	BDE VALIDATOR'S SIGNATURE 
USAREC FORM 25-1.1, 14 NOV 2018 V 1.00	

Figure 2- 1 Validation of Telephone bills (USAREC Form 25-1.1)

2-7. Strategic Planning.

Planning for the effective use of IM/IT is an ongoing activity and the responsibility of every commander/director within USAREC. IM/IT plans provide the commander visibility over IM requirements and assist the USAREC CIO in enterprise planning and acquisition, standards application, and overall fiscal responsibility. The USAREC IM/IT Strategic Plan lays out the strategic direction and priorities of IM/IT in the command and will be updated by the USAREC CIO annually.

Figure 2- 2 Communications Relocation Checklist

Communications Relocation Checklist		
<p>Network installation can take up to 120 days, and telephone installation can take up to 60 days. This time starts when USAREC receives the request for service (RFS). The unit understands/assumes the risk of moving into a new location without network services if the RFS is received by G6 within 120 days of move in. There must be a signed lease for work to begin on the new location. This checklist must accompany any Request for Service.</p>		
S-6 NAME:	S-6 EMAIL:	S-6 PHONE:
DATE LEASE SIGNED:	SCHEDULED MOVE-IN DATE:	RSID:
Pre Move-in Checklist: Conduct site survey and check the following:		REMARKS
1. What communications services are currently available at this location? <input type="checkbox"/> Fiber Optic Cabling <input type="checkbox"/> Copper <input type="checkbox"/> None NOTE: If "none" is selected, contact your facility manager immediately.		
2. Does the building owner require specific vendors for communication/network services?		
3. Is there sufficient cellular coverage to support the operation of phones and Mifi devices?		
4. If this is a multi tenant building, what cellular services do they use?		
a. What service providers do they use?		
b. What type of equipment do they use?		
c. Do other tenants experience interruptions in service for any reason?		
Post Move-in Checklist: Retain a copy of this checklist to use during move-in inspection.		REMARKS
1. Can all users connect to station wireless?		
2. Is station address correct in HSS?		
3. Ensure HSS reflects correct personnel.		
4. Contact HRC to add MFD (printer) to: network.usarmy.knox.hrc.list.persinsd-winops-server-spt		
5. Contact CSD (usarmy.knox.usarec.list.hq-g6-biometrics-team) to update Livescan information.		
6. Check all phone lines and fax line for correct operation.		
7. Ensure all personnel order business cards reflecting new address and phone number. https://soc.stationeryorders.com/usarec/login.asp		
All Relocations, Expansions, New Builds Required Signatures		
BN S-6 Information Officer	Name <input type="text"/>	Signature <input type="text"/>
BN S-4 Facility Officer	Name <input type="text"/>	Signature <input type="text"/>
Relocations scheduled less than 120 days from Date of Lease signing		
I acknowledge there is less than 120 days between lease signing and scheduled move in date. I acknowledge risk that the communications capability may be effected by this timeline.		
Company Commander	Name <input type="text"/>	Signature <input type="text"/>
Battalion Commander	Name <input type="text"/>	Signature <input type="text"/>
USAREC Form 25-1.2, 27 Mar 19		V1.10
(This is a new form)		

Figure 2- 2 Communication Relocation Checklist (USAREC Form 25-1.2)

2-8. IT Asset Management Program.

a. The ITAM program provides for the management of IT assets, including contracts and licenses. USAREC will ensure compliance with contractual obligations, and provide maximum efficiency and use of IT assets.

b. Accountability for compliance with this program rests with the DCG-S, USAREC and commanders at all levels. The CIO/G-6 and S-6 staffs are responsible for the execution, enforcement and oversight of the ITAM program. The program is applicable to all personnel assigned, or, attached to the command, including other personnel utilizing USAREC IT assets with the approval of the CIO, USAREC.

c. The G-6 and S-6 staffs will ensure compliance with the ITAM program, and will implement the program to support their Commanders, staffs, and personnel within their organizations.

d. IT assets are defined as any hardware, software or service that directly supports the prospecting, processing, or enlistment accessions of soldiers.

e. The ITAM program is not a property accountability program, but is complimentary to those functions. The ITAM program does not supersede or intervene with the Command Supply Discipline Program.

f. IKROme will be the key management tool for IT assets assigned to organizations and individuals. USAREC personnel are responsible for updating the “MyProfile” app in the drop-down menu in IKROme.

g. Detailed information regarding the ITAM program and its implementation are outlined in USAREC Pam 25-1-1.

Chapter 3

Capital Planning and Investment Management.

3-1. Portfolio Management Overview.

The primary goal of IM/IT Capital Planning and Investment Management is to prioritize IM/IT spending across USAREC functional proponents by assessing and managing IT as a portfolio of investments. The APMS is the Army’s primary portfolio management decision support tool. Effective portfolio management ensures that IM/IT investments support the Army’s mission, vision, and goals; ensures an efficient delivery of capabilities to the warfighter; and maximizes return on investment to the enterprise. APMS assists USAREC CIO in identifying potential redundant or inefficient systems for consolidation or elimination, while supporting budgeting decisions.

3-2. Developing a Business Case.

The business case defines the purpose and expected outcome of the initiative. A business case is used by the USAREC CIO and RRB to assess the value of proposed IM/IT projects (initiatives) and make a recommendation on funding and priority. The level of detail required for the business case is in direct relationship to the cost of the initiative. A fully developed business case includes the purpose, costs, recommended solution, operational impact, risk assessment, funding plan, milestones, and performance measures. USAREC IM/IT acquisitions or initiatives costing \$50K or more over the project lifecycle will have a fully developed business case and must be sponsored at the directorate level.

3-3. Milestone Reviews.

Initiatives costing more than \$500K over their lifecycle must include annual milestone reviews during the development stage and after implementation, during sustainment. The RRB will conduct a review to assess the accuracy of cost estimates and implementation timelines, the satisfaction of business users with the results of their investment, the achievement of benefits that were stated, and to gauge whether any lessons were learned. The annual milestone review meeting of the RRB will be in the first quarter of the fiscal year.

3-4. Submitting Capability Requests.

USAREC organizations with a business requirement that do not have a recommended technical solution require CIO assistance using the ITEPS form. CIO will work with the submitting organization to build the appropriate level of business case and identify the best solution to meet the requirement.

3-5. Resource Management.

HQ USAREC G4/8 manages all requirements throughout the PPBES cycle and the accompanying current and budget year unfunded requirements (UFR) process, to include requirements that depend upon IM/IT for their total or partial solution. G4/8 coordinates with USAREC CIO regarding the validity, architectural conformance, duplication, and priority of requirements for IM capabilities. CIO coordinates with USAREC organizations to clarify, consolidate, or de-conflict requirements they have submitted to G4/8 for funding consideration. USAREC CIO recommends strategies for integrated management of IM/IT investments to the RRB.

3-6. Types of Funds.

- a. The two categories of funds that generally fund IT are OMA and OPA.
- b. OMA is used if the cost of an IM/IT system is below the investment threshold mandated by public law (currently \$250K). Acquisitions will not be fragmented to stay below this threshold for a system.
- c. OPA is used if the cost of an IM/IT system exceeds \$250K and should be programmed 2 years out in the POM. IAW Defense Finance and Accounting Service-Indianapolis Center (DFAS-IN) Manual 37-100 Appendix A, an IM/IT system exists if a number of components are designed primarily to function within the context of a whole and will be interconnected to satisfy an approved Army requirement. This appendix also provides guidance on what should be included when calculating the total cost of a system to determine if IM/IT exceeds the OMA/OPA threshold.

3-7. Validated UFRs.

UFRs are generally not written with the specificity required for approval of IM/IT acquisitions. Therefore, the requiring activity must complete an ITEPS form prior to CIO consideration of the UFR.

3-8. IM/IT and Telecommunications Acquisitions.

Requests for acquisition of IM/IT are submitted via the ITEPS and the governance processes previously described in chapter 2, para 2-3 apply. Services related to IM/IT are considered as part of the oversight requirement of this regulation.

a. Requiring activities must obtain USAREC CIO approval via the ITEPS form for acquisition of IM/IT that meets any of the following criteria:

- (1) All software initiatives including COTS modifications.
- (2) All hardware and software, network, wireless, and security devices (also referred to as IT assets).
- (3) All collaboration software and any other software not on the service providers recommended product list.
- (4) Any software, hardware (including maintenance), and services not being purchased using mandatory CHES contracts or that do not have a CHES statement of Non-availability.
- (5) Any hardware, software, IM/IT initiatives, or services with a cumulative cost above \$3K.
- (6) Consumables or general supply/support items, i.e., compact discs, digital video disks, tapes, ribbons, ink/toner cartridges, bulbs, publications, cables, and carrying cases. Local IM/IT policy will address these items.
- (7) Automated components embedded as part of a system, medical instrumentation, and servo-mechanisms that do not interface or communicate outside the host tool, system, or device. These systems must meet DA and DOD reporting requirements.
- (8) IT assets are defined as IT Hardware/equipment directly effecting prospecting, processing, enlisting and assessing a Soldier. The BOIP is a planning tool of procurement actions/further Program Objective Management (POM) requirements and other financial forecasting tools supporting the USAREC IT Asset Management Program.
- (9) IT assets will be accounted for in Headquarters Support System (HSS) for assignments to individuals and organizations. The use of HSS for IM/IT assets does not supplement or circumvent the Army Command Supply Discipline Program or other logistics management or property accountability programs as directed by Army directives/regulatory guidance.

b. IM/IT Acquisition supporting the BDE/BN automation data processing equipment (ADPE) will be executed IAW process outlines in USAREC Pam 25-1-1.

c. Telecommunications. USAREC CIO centrally manages the command's long haul communication requirements. Long haul communications are any general or special purpose telecommunications leaving the installation, regardless of distance. USAREC CIO will coordinate with organizations annually to validate long haul requirements.

(1) Long haul services are categorized in one of two ways: Defense Information System Network (DISN) or non-DISN.

(a) DISN subscription services include Defense Switched Network, Defense Red Switch Network, Joint Worldwide Intelligence Communication System (JWICS), Non-secure Internet Protocol Router Network (NIPRNET), Secret Internet Protocol Router Network (SIPRNET), Defense Messaging System (DMS), Ground Surveillance Radar, Intelligence, Surveillance and Reconnaissance, Video Teleconference, and DISN transport services. DISN services are programmed for and paid by DA.

(b) Non-DISN long haul includes services for commercial and military satellite services, Global System for Mobile Communication, Federal Telecommunications Services, and Public Switch Telephone Network. Non-DISN services are programmed and paid for by USAREC CIO.

(c) Start, Change, or Discontinue Long Haul Service. USAREC organizations coordinate the provision of service with the supporting NEC (Network Enterprise Center) who enters the request through Defense Information Systems Agency Direct Order Entry (DDOE). Long haul service requests specific to USAREC mission support (whether DISN or non-DISN) are automatically routed through USAREC CIO for approval by the DDOE web application. New DISN services must be paid for by USAREC in the year of execution until programmed by DA. New non-DISN services are added to the program requirements by USAREC CIO.

(2) Cell Phones and Smart Devices. AR 25-1 and AR 25-2 govern policies and procedures for cell phones and Smart devices (e.g., smartphones). Commanders or directors must have a program in place to actively manage the use of wireless technology to include:

(a) Developing local allocation priorities in IAW G6 Equipment IT Basis of Issue Plan (BOIP).

(b) Assigning responsibilities for reviewing expenditures and usage, and evaluate opportunities for resource sharing, use of aggregate purchases, and pooling of minutes.

(c) Implementing ongoing asset tracking and inventory control of these devices.

d. Copiers. AR 25-30 governs the policies and procedures for self-service copying management.

e. Requests for copiers are submitted via the ITEPS system and reduction in print directive guidelines apply. USAREC organizations will utilize enterprise lease copier contracts to reduce print requirements and associated costs.

3-9. Contracts.

a. Contracts supporting IM/IT based systems must include wording that requires compliance with Army IA requirements, such as system certification, accreditation, and net-worthiness; training and certification of IA personnel; and IAVM compliance. These requirements must be included in mission needs statements, operational requirements documents, capstone requirement documents, statements of work, and all other system acquisition, contracting, and development documents.

(1) USAREC contracts will require all software or systems developed for use on the Army Enterprise Info structure (AEI) to meet minimum security standards stated in AR 25-2 and other DA and DOD policies, to include IAVM compliance, patch management, and the use of antivirus and other IA software.

(2) All information systems developed or acquired must meet DOD and DA certification, accreditation, and/or net-worthiness requirements before being connected to the AEI.

(3) Contractor nominated personnel must meet all IA training and certification requirements in AR 25-2, DOD 8570.01-M, and the Army's IA Training Best Business Practices before acceptance for employment. Additionally, contractors must maintain Army IA training and certification compliance throughout the contract period at no expense to USAREC.

(4) Contractor nominated personnel must meet security clearance requirements specified in AR 25-2 before acceptance for employment. Contractors must maintain their security clearances throughout the contract period at no expense to USAREC.

(5) Contractor access to information residing on a government information system (IS) or network will be limited to that required to fulfill the terms of the contract.

(6) Contractor owned and operated IS will meet all security requirements for government owned hardware and software when operating on the AEI or conducting official business.

b. In accordance with DA PAM 25-1-1, all COTS IT hardware, software (to include maintenance) and services must be purchased from CHES contracts that include the Enterprise Software Agreements (ESA). If the requirement cannot be fulfilled via these contracts, request a waiver from CHES. The process is for government personnel to submit IT purchases from their contracts. Turn-key service contract, initiated by or for USAREC, will not include tasks and related dollars for the contractor to purchase COTS IT hardware or software. If the CHES Office preferred purchasing process cannot be met:

(1) The Contracting Officer for the services contract must write an authorization letter to authorize the contractor to purchase COTS IT from the CHES contracts on behalf of the government.

(2) The contractor must have CAC to access the CHES site.

(3) The contractor must be able to make the specific types of payment required by the CHES contracts such as delivery order, credit card, or check.

(4) Use of a contractor for purchase of COTS IT does not void the requirement for USAREC and Army mandated approvals before the actual purchases are made.

c. Contractors must abide by local installation policies for network and telephone access. Contractor equipment cannot be connected to networks without service provider approval. Contracts requiring access to government furnished equipment must state that local installation policies for internet access will be met.

Chapter 4 Knowledge Environment.

4-1. General.

The knowledge environment concerns the information USAREC requires to execute its missions in support of the Army and the DOD. The requirements for content management and web design contained in this chapter also apply to the USAREC public web presence.

IT assets will be accounted for as Headquarters Support System (HSS) for assignments individuals and organizations. The use of HSS for IM/IT assets does not supplement or circumvent the Army Command Supply Discipline Program or other regulatory guidance regarding logistics management/property accountability programs.

4-2. Collaboration Capabilities.

The DOD and Army imposes extra conditions on the management of collaboration capabilities and the CIO enforces these requirements for USAREC mission collaboration needs. Collaboration capabilities enable two or more individuals who are not collocated to use an electronic environment to communicate, plan, coordinate and make decisions. They include, for example, voice and video conferencing; text, document, and application sharing; awareness and instant messaging; and white boarding. CIO develops and maintains architecture for collaboration capabilities and coordinates the service delivery responsibilities. CIO advises USAREC organizations on solutions for their unique collaboration requirements and approves the acquisition of new collaboration capabilities, regardless of cost. USAREC organizations will:

a. Utilize existing solutions such as AKO, TRADOC Knowledge Environment (TKE), Battle Command Knowledge System (BCKS), DCS, MilSuite and Global Video Services (GVS).

(1) AKO (<https://us.army.mil>) is the Army's intranet and the preferred collaboration capability.

(2) TKE is a TRADOC-hosted portal that provides close integration with MS Office products to enhance organizational productivity (<https://tke.army.mil/default.aspx>). TKE site owners can authorize foreign officials and students assigned to USAREC access to TKE.

(3) BCKS provides a network of structured professional forums (SPF) focused on knowledge transfer and leader development (<https://bcks.army.mil>). Creating a SPF community on BCKS provides a complimentary capability to the training and leader development mission of the schools.

b. Utilize DOD and Army approved products and contracts, <https://ascp.monmouth.army.mil/scp/index.jsp>, and TRADOC-specific extensions of these.

c. Obtain certifications or waivers at the required level for alternative solutions IAW current guidance on the Employment of Collaborative tools <https://www.us.army.mil/suite/doc/5747635>.

d. Propose modifications to enterprise collaboration capabilities, e.g., AKO and TKE, via the USAREC CIO representative to the configuration control boards.

4-3. Content Management.

Access to relevant content is the underpinning of the knowledge environment. USAREC organizations and offices with web pages, portals, repositories, and shared drives will adhere to the following policies to maximize the security and accessibility of their content.

a. Storage. AKO is the preferred access point and storage for content. USAREC organizations will not use e-mail to transmit large files and attachments and will comply with size limitations identified by service provider. Sharing of large files should be done using AKO files, TKE, U.S. Army Aviation and Missile Research Development and Engineering Center Safe Access File Exchange (AMRDEC) SAFE, or another secure file sharing environment. USAREC activities are authorized to store content in a variety of repositories:

(1) AKO Files. All organizations will have a Knowledge Center on AKO and use it for content that must be available to the Army community. USAREC CIO determines the AKO organizational file structure at the Army command level. Each top level organizational community in USAREC will create at least one Knowledge Center and public folder that is searchable and accessible to all official personnel.

(a) Public Folders. The AKO public folder only includes content that is available to all official personnel and for which the organization is the proponent and release authority.

(b) Workgroup/Limited Access Folders. These folders are managed by the folder owner who grants access to users or groups based on mission requirements. These folders may be used for copies of official documents or publications needed on a temporary basis by the members of the group. Copies will be deleted by the folder owner when no longer needed.

(2) USAREC Shared Drives. Shared drives do not support a net-centric architecture and USAREC activities will make

limited use of them only as required for local and temporary processes. Authorized uses include as records management archives, web development environment, or for short term storage when transferring content.

(3) Databases. USAREC does not own and will not establish local databases outside enterprise solutions.

(4) Web sites and Portals (including TKE, AKO and BCKS).

(a) TKE is appropriate for development and sharing of internal USAREC organizational content. TKE content is web-accessible.

(b) Content on web sites and portals will be linked to the authoritative source, rather than copied or duplicated on site.

(c) Content on public web sites must be approved for release by the PAO.

(d) All non-public content will be on a site that is accessible through AKO authentication, common access card (CAC) authentication, and/or restricted by user name and password.

b. Content Security. Data owners must determine the level of accessibility for their content, i.e., public or limited.

Working draft content will not be stored in publicly accessible files or portals.

(1) The following sources and types of information must not be made publicly accessible:

(a) Training support plans, mission training plans, drills, field manuals, tactical vignettes, and other material that describes how Soldiers perform functions in the U.S. Army. Examples include small unit tactics patrolling, stability and support operations, engineer operations, aviation operations, logistics procedures, and systems capabilities.

(b) Specific vulnerabilities to operations, equipment, or personnel, including, but not limited to, force protection, significant troop movements, readiness data, and tactics, techniques, and procedures (TTP).

(c) Lessons learned, formal and informal TTP, and "how-to" articles that deal with topics described in paragraphs (a) and (b) above.

(d) Press releases that detail how Soldiers are accomplishing the mission.

(e) Information relating to the funding, fielding, vulnerabilities, and capabilities of new equipment.

(f) Classified information is to be secured IAW [AR 380-5](#) and not to be made accessible from any UNCLASSIFIED server or web site, to include private web sites or portals.

(2) Unclassified critical and sensitive operational traffic that specifically includes information about "shortfalls in training" due to funding, general officers' overseas travel schedules, and deployed/deploying troops will be transmitted over a secure network. USAREC organizations will use the following guidance regarding the classification and transmission of operational data:

(a) Data classified as "For Official Use Only" will, at a minimum, be signed using CAC/public key infrastructure (PKI).

(b) Data classified as "Sensitive but Unclassified" will, at a minimum, be signed and encrypted using CAC/PKI.

(c) Data classified as "Confidential" or "Secret" will be transmitted over a network with a minimum-security classification of Secret (e.g., SIPRNET, JWICS).

(3) USAREC activities will periodically review their secure network capabilities to ensure they are capable of implementing the above guidance. USAREC organizations will coordinate with their supporting DOIM regarding access to classified long-haul networks available as common user (non-reimbursable) services. USAREC organizations will report additional requirements for secure network capabilities to the USAREC CIO using the RAD form.

c. Content Discoverability. USAREC organizations will implement Army policies regarding the organization of content and its discoverability, e.g., standard metatags and taxonomies.

(1) USAREC organizations will use the DOD mandatory discovery metadata elements for resources posted to community and shared spaces as identified in the Department of Defense Discovery Metadata Specifications (DDMS) (Appendix C). The DOD Metadata Registry and Clearinghouse is a catalogue of XML schemas, taxonomies, reference data sets, and data elements. Metadata schemas and taxonomies for USAREC content that need to be accessed across the DOD enterprise will be registered in the DOD Metadata Registry and Clearinghouse <https://metadata.dod.mil/mdrPortal/appmanager/mdr/mdr>.

(2) USAREC organizations will utilize the Sharable Content Object Reference Model (SCORM) when developing learning content. SCORM is a suite of technical standards that enable web-based learning systems to find, import, share, reuse, and export learning content in a standardized way. SCORM is written primarily for vendors and toolmakers who build learning management systems and learning content authoring tools so they know what they need to do to their products to conform with SCORM technically. For details on SCORM, access the following URL <http://www.adlnet.gov/index.cfm>.

4-4. Records Management.

USAREC commanders will establish a records management program IAW U.S. Code: Title 44, Chapter 31. Records management applies to the entire lifecycle of official records from creation through final disposition. Official records include all documentary materials, regardless of physical form or characteristics that provide evidentiary accounting for decisions, policies, plans, organizations, functions, procedures, operations, and essential transactions of an organization. It is the originating organization's responsibility to determine the record status of information and manage it appropriately. USAREC organizations must implement Army policies regarding the management of official records per AR 25-400-2.

The Army Records Information Management System (ARIMS) is a web-based tool to manage both hard-copy and electronic Army records.

a. USAREC Records Management Duties and Responsibilities (see Table 4-1)

b. E-mail has become a primary means of communicating decisions, policies, plans, procedures, and other essential information regarding government business; and, therefore must be preserved. E-mail, identified as records, must be managed, protected and retained as long as needed for ongoing operations, audits, legal proceedings, or research IAW AR 25-400-2 and ARIMS Record Retention Schedule-Army. Individuals originating the e-mail will determine the record status of their e-mail.

(1) E-mail records might include: Policies and directives; correspondence or memoranda related to official business; work schedules and assignments; agendas and minutes of meetings; drafts of documents that are circulated for comment or approval; any document that initiates, authorizes, or completes a business transaction; and final reports or recommendations.

(2) E-mail records identified with retention of 6 years or less are designated as keep ("K") records and managed locally through the lifecycle. E-mail records identified with retention longer than 6 years are to be designated as transfer ("T") records and transferred to the ARIMS Army electronic archive records repository. These records will be further managed and disposed of at the end of their lifecycle or transferred to the National Archives and Records Administration as a permanent record.

(3) The following examples are generally not considered in the category of e-mail records: Personal messages and announcements not related to official business; copies of extracts of documents distributed for convenience or reference; and announcements of social events (e.g., retirement parties or holiday celebrations).

c. Per AR 25-11, paragraph 13-3a, routine, unclassified organizational record information may be sent in memorandum format as an attachment via organizational e-mail. Organizational e-mail accounts are the preferred method for passing official tasking's, official requests, and official responses. Messages containing record information should be digitally signed using the organizational e-mail account's PKI certificate. Organizations can obtain certificates for their organizational accounts from the Army Registration Authority, army.ra@us.army.mil.

4-5. Portal/Web Site Administration.

This paragraph provides policy specific to creating and maintaining a USAREC web site or portal. USAREC activities will determine their local requirements to produce and maintain a site and coordinate their establishment with the CIO/G6 or S-6 and appropriate webmaster. The person responsible for maintaining public web sites is known as the mission webmaster and the person responsible for maintaining a portal is known as the portal administrator. All USAREC public sites must have a primary mission webmaster or portal administrator designated in writing by a commander/supervisor. All USAREC public and private web sites, except those operating under unified cloud capabilities, must be located on a .mil domain. Pre-existing Army web sites maintained in non-government domains (i.e., .org, .com, .net, and .edu) will execute plans to transition web sites to a .mil domain.

a. Mission Webmaster/Portal administrators will—

(1) Ensure sites comply with DOD web site administration policy, AR 25-1, and subsequent DOD and Army directives. Current policy can be found at <http://www.defenselink.mil/webmasters/> and <http://www.army.mil/webmasters/>.

(2) Establish a process for the periodic review of their sites for security risks and design deficiencies.

(3) Ensure their web sites maintain a consistent look and feel and that all web pages clearly identify which web site the visitor is on.

(4) Monitor the accuracy of links on their web sites. At least monthly, mission webmasters will review error data in their web site's automated access logs and take action to correct link and document access errors.

(5) Complete the Online Army Webmaster Training Course located at <https://iatraining.us.army.mil/index.php>.

(6) Perform housekeeping functions such as monitoring file expiration and cleanup; and for limited access sites, deleting users who no longer need access to the portal.

(7) A statement indicating "This is an official U.S. Army site."

Table 4-1 USAREC Records Management Duties and Responsibilities

USAREC Records Management Duties and Responsibilities

TITLE	APPOINTED LEVEL	DUTIES AND RESPONSIBILITIES
Records Administrator (RA)	USAREC CIO	An individual who is appointed in writing and serves on the Army Command or Army Staff (ARSTAF) with command-wide records management program responsibilities. RAs have approval authority for AOs and RCs requesting RM or RHAM privileges. RAs may approve Office Records List (ORL) and serve as points of contact (POC) for the access and release of stored records for which they are responsible (See <u>para 8-2g(3), AR 25-1</u>)
Records Holding Area Manager (RHAM)	Garrison	An individual whose duties include managing and directing the operations of a records holding area facility. RHAMs may also possess the same duties and access privileges as a Records Manager if they have been approved by their Army Command Records Administrator (RA). (See <u>para 8-2g(7), AR 25-1</u>).
Records Manager (RM)	Member designated by the USAREC CIO	An individual serves at the subordinate command level or on the installation garrison staff with command-wide or garrison-wide records management responsibilities. RMs have approval authority for AOs requesting RC privileges. RMs also approve proposed ORL and serve as (POC) for the access and release of stored records for which they are responsible. (See <u>paras 8-2g(4), 8-2g(6), and 8-2g(7), AR 25-1</u>).
Records Coordinator (RC)	As needed to assist RMs	RCs are responsible for providing Records Management services to one or more unit(s)/office(s) and act as liaison between the unit(s)/office(s) and the servicing RM and Records Holding Area Manager. They also serve as POC for the access and release of stored records for which they are responsible. (See <u>para 8-2g(8), AR 25-1</u>).
Action Officer (AO)	As needed to meet needs of individual organization	AOs are responsible for managing the records they create on behalf of the Army that are used for their unit/office level business operations. An AO can use ARIMS to create proposed ORL to categorize the records created in his/her office. (See <u>para 8-2g(9), AR 25-1</u>).

37-1* Coordinate with USAREC Records Administrator for additional RMs to support the needs of the organization.

Table 4- 1 USAREC Records Management Duties and Responsibilities

b. **Public Sites.** Public sites are developed when an organization wishes to provide all users with information. There are two types of public sites USAREC public web sites and AKO organizational portals.

(1) **USAREC Public Web Sites.** Organizations will coordinate the establishment of new web sites and Uniform Resource Locators (URLs) with the next higher level webmaster who will coordinate with the USAREC PAO, the mission PAO, OPSEC officer, and SJA. PAOs must clear information for posting on public web sites. When requested by PAOs, the OPSEC officer and SJAs will assist in information reviews. USAREC personnel will not make Privacy Act (PA) or Freedom of Information Act (FOIA) exempt information accessible using public web sites.

(2) **AKO Organizational Portals.** Organizational portals will be created under the appropriate USAREC organization as detailed in TR 10-5 series. Organizations desiring to create a new portal will coordinate with the USAREC AKO administrator. Organizational portal administrators are responsible for the organizational structure under them to include authorizing and creating of sub-communities and knowledge centers. Sub-community administrators are responsible for notifying the next higher organization level administrator of changes in personnel and for maintenance of the structure under them.

c. **Restricted Access Portals.** Administrators are responsible to ensure all content inappropriate for public viewing is located behind AKO or the approved USAREC knowledge environment. Restricted access by domain or Internet Protocol address only (i.e., .mil restricted) is not sufficient for content inappropriate for public viewing. Once an administrator has been designated, the administrator of the portal is responsible for assigning all other rights/permissions for users granted access. There are several options for restricted access portals in USAREC: AKO Team Sites, TKE, and BCKS.

Chapter 5 Network Operations.

5-1. RSN-Provided Infrastructure.

The HRC IT service provider provides common user baseline services (e.g., NIPRNET and SIPRNET, e-mail, file storage, print, web, and domain services) for USAREC. The USAREC CIO will assist USAREC organizations in the resolution of infrastructure issues, e.g., with the IT service provider that cannot be resolved locally.

5-2. Mission Support.

Common and mission servers will be consolidated or eliminated where operationally possible in order to lower the total cost of operating. USAREC will centralize mission IM/IT services in common hosting facilities under the supervision of an approved service provider, when feasible. USAREC elements with new or emerging requirements for IM/IT services will report them via the ITEPS system. When planning for new requirements, incorporate maximum use of existing Army and USAREC capabilities before considering alternative solutions.

5-3. Network Access.

a. Except where the IT service provider provides community of interest network access via other means. USAREC activities will maximize the use of IT service providers' network access services. USAREC activities will not circumvent or duplicate the network access architecture the service provider operates and maintains.

b. USAREC organizations will access the Internet only through the RSN. USAREC organizations will not acquire services from commercial Internet service providers without meeting requirements of AR 25-1. All web sites and web-enabled applications will be hosted on Army or DOD-operated systems. USAREC units will coordinate with G6 provider for alternate means of support/access (i.e., VPN) if DOD networks are unavailable at their location.

c. USAREC personnel and students who use personal home computers to access government sites for work or professional development, e.g., Outlook Web Access, Distance Learning, AKO, may require CAC cryptographic log-on to access these sites. Organizations are authorized to issue CAC readers and middleware purchased at government expense for home use. This equipment is government property and will be returned when no longer needed.

d. USAREC does not permit the provision of network services for telework. TRADOC Regulation 600-18 prescribes TRADOC's general policies for telework. Information Management Officers will coordinate provision of network services to teleworkers.

5-4. Wireless Networks.

Wireless networking removes the encumbrance of wire connections on portable devices and provides users the ability to travel beyond traditional network boundaries without losing network connectivity. Organizations desiring to implement wireless solutions must submit requirements via the ITEPS form and develop the business case that identifies cost benefit, security, operational necessity. USAREC organizations must program funding for this network capability. Wireless local area network solutions must be implemented IAW the policies and procedures in AR 25-2 and Army's Wireless Security standards Best Business Practice.

5-5. Appropriate Use of Communications Systems.

The use of communications systems involving e-mail is limited to the conduct of official business or other authorized uses as defined in AR 25-1.

a. Official business as it concerns e-mail message use is defined as those necessary in the interest of the government (i.e., e-mail messages that directly relate to the conduct of DOD, DA, or USAREC business or that have an indirect impact on the command's ability to conduct its business). Signature blocks for official e-mail messages should only include the sender's name, title, organization, phone, fax, and e-mail address. Unless as otherwise noted below, unofficial logos, sayings, quotations, mottos, slogans, or similar messages or attached unofficial pictures or files are not permitted for use in official e-mail traffic, either as part of the signature block or located elsewhere within the official e-mail message. The only exception for the conduct of official business involving e-mails is the inclusion of recognized unit or USAREC organizational mottos or logos (such as "Provide the Strength").

b. Authorized use (as opposed to official use) e-mail messages are not similarly restricted by format concerns as it relates to the use of logos, sayings, quotations, mottos, slogans, or similar messages; however, there are prohibitions in place regulating the conduct of authorized use of e-mail for unofficial purposes. Prohibited use of USAREC communications systems include:

(1) The use of communications systems that would adversely reflect on DOD, DA, or TRADOC (such as those involving sexually explicit e-mail or pornographic images; chain e-mail messages; unofficial advertising, soliciting, or selling via e-mail; and other uses that are incompatible with public service).

(2) Political transmissions to include transmissions that advocate the election of a particular candidate for public office.

5-6. Command, Control, Communications & Computers (C4) Reporting.

Commanders will ensure C4 degradations affecting Military Entrance Processing Centers, Battalion or Brigade HQs via Commander Critical Information Requirements (CCIR) to the Command Operations Center as prescribed by UR 190-4.

Chapter 6 Cybersecurity

For information, see USAREC Reg 25-2 "USAREC Cybersecurity".

Appendix A References

Section I Required Publications

AR 25-1

Army Information Technology

AR 25-2

Information Assurance

AR 25-30

Army Publishing Program

AR 25-400-2

The Army Records Information Management System (ARIMS)

DA PAM 25-1-1

Army Information Technology Implementation Instructions

UR 25-2

USAREC Cybersecurity

Section II Related Publications

DOD Instruction 5000.2

Operation of the Defense Acquisition System

DFAS-IN Reg 37-1

Finance and Accounting Policy Implementation

(<https://dfas4dod.dfas.mil/centers/dfasin/library/ar37-1/>)

AR 5-14

Management of Contracted Advisory and Assistance Services

TR 10-5

TRADOC Organization and Functions

DOD Instruction 8500.1,

Cyber Security

Section III Prescribed Forms

UR 25-1.1

Validation of Phone bills

UR 25-1.2

Communications Relocation Checklist

Section IV Referenced Forms

There are no items in this section.

Appendix B Metadata and Taxonomies

Department of Defense Directive 8320.2 - Data sharing in a Net-Centric Department of Defense, establishes policy and responsibilities to implement data sharing and to make data visible, accessible, and understandable.

The DDMS defines discovery metadata elements for resources posted to community and shared spaces. The DDMS specifies a set of information fields that are to be used to describe any data or service assets that are to be made known to the DOD Enterprise. The most recent version of DDMS will be employed consistently across the department's disciplines, domains, and data formats.

DDMS Tags (*Mandatory):

- Security* - The highest level of classification.
- Title* - A name given to the content resource.
- Identifier* - An example of an identifier is a URL or standard serial number.
- Creator* - An entity primarily responsible for making the content of the resource, i.e. author.
- Publisher - The entity responsible for posting the authoritative content.
- Contributor - An entity responsible for making contributions to the content of the resource.
- Date - A date of an event in the lifecycle of the resource (YYYY-MM-DD).
- Rights - Information about rights held in and over the resource (e.g., copyright or intellectual property rights).
- Language - A language of the intellectual content of the resource.
- Type - Name of the taxonomy schema used.
- Source - A reference to the original resource from which the present resource is derived.
- Subject* - Topic(s) of the content of the resource.
- Geospatial Coverage* - Geographic place names or coordinates that relate to the resource, mandatory unless not applicable.
- Temporal Coverage* - Subject matter coverage expressed in terms of one or more periods of time, mandatory unless not applicable.
- Virtual Coverage - The subject matter coverage of a publication in terms of one or more virtual addresses.
- Description - A summary of the content.
- Format - The physical or digital manifestation/media type of the resource (i.e., video, mime, Word document, etc.)

Glossary

Section I Abbreviations

ACC

Army Contracting Command

ADPE

Automated Data Processing Equipment

AEI

Army Enterprise Infrastructure

AITR

Army Information Technology Repository

AKM

Army Knowledge Management

AKO

Army Knowledge Online

APMS

Army Portfolio Management System

AR

Army Regulation

ARCIC

Army Capabilities Integration Center

ARIMS

Army Records Information Management System

BCKS

Battle Command Knowledge System

BMMP

Business Management Modernization Program

BOIP

Basis of Issue Plan

BPA

Blanket Purchase Agreement

CB

Consolidated Buy

CG

Commanding General

CIO

Chief Information Officer

COTS

Commercial Off-The-Shelf

CHESS

Computer Hardware Enterprise Software & Solution

C4

Command, Control, Communications, & Computers

DA

Department of the Army

DCG

Deputy Commanding General

DCSOP & T

Deputy Chief of Staff for Operations and Training

DCSRM

Deputy Chief of Staff for Resource Management

DDMS

Department of Defense Discovery Metadata Specifications

DDOE

Defense Information Systems Agency Direct Order Entry

DFAS-IN

Defense Finance and Accounting Service-Indianapolis Center

DISN

Defense Information System Network

DMS

Defense Messaging System

DOD

Department of Defense

EA

Enterprise Architecture

EAP

Enterprise Architecture Plan

EAMB

Enterprise Architecture Management Board

ERB

Enterprise Review Board

FISMA

Federal Information Security Management Act

FOUO

For Official Use Only

HQ

Headquarters

HQDA

Headquarters, Department of the Army

HTTP

Hyper Text Transfer Protocol

IA

Information Assurance

IAVM

Information Assurance Vulnerability Management

IAW

In Accordance with

IM

Information Management

IMA

Installation Management Agency

IM/IT

Information Management/Information Technology

IMO

Information Management Officer

IMSP

Information Management Strategic Plan

IS

Information System

IT

Information Technology

ITAM

IT Asset Management

ITEPS

Information Technology Equipment Procurement and Service

JWICS

Joint Worldwide Intelligence Communications System

KM

Knowledge Management

LCR

Life Cycle Replacement

MRB

Mission Resources Board

MSC

Major Subordinate Command

NETCOM

Network Enterprise Technology Command

NIPRNET

Non-secure Internet Protocol Router Network

OMA

Operations Maintenance Army

OPA

Other Procurement Army

OPFAC

Operational Facilities

OPSEC

Operational Security

PAM

Pamphlet

PKI

Public Key Infrastructure

POM

Program Objective Memorandums

PPBES

Planning, Programming, Budgeting and Execution System

RAD

Reporting and Requisition Decision

RRB

Requirements Review Board

SBU

Sensitive But Classified

SCORM

Sharable Content Object Reference Model

SIPRNET

Secure Internet Protocol Router Network

SJA

Staff Judge Advocate

SME

Subject Matter Expert

SPF

Structured Professional Forums

SRC

Senior Resource Committee

TKE

TRADOC Knowledge Environment

TR

TRADOC Regulation

TRADOC

Training and Doctrine Command

TTP

Tactics, Techniques, and Procedures

UFR

Unfinanced Requirement

URL

Uniform Resource Locator

VPN

Virtual Private Network

Section II Terms**Authoritative Data Source**

A source of data or information that is recognized to be valid or trusted because IM/IT is from an official release authority or an official publication or reference (i.e., regulation or doctrine).

Content Management Collection

A set of processes and technologies that support the evolutionary life cycle of digital information.

Data Management

The process of creating a basis for posting, sorting, identifying, and organizing the vast quantities of data available to DOD. (AR 25-1)

Discovery

Services that enable the formulation and execution of processes to advertise (make visible) and locate data assets (e.g., files, databases, services, directories, web pages, streams) by exploiting metadata descriptions stored in and or generated by IT repositories (e.g., directories, registries, catalogs, repositories, other shared metadata storage) and other exposed product or service attributes.

Disposition instructions

Precise instructions specifying the time or event for transfer, retirement, or destruction of records.

Federated Data

Data that is accessed across physical boundaries, which may be system to system, department to department, or enterprise to enterprise boundaries.

Information life cycle management

A comprehensive approach to managing the flow of an information system's data and associated metadata from creation and initial storage to the time when IM/IT becomes obsolete and is deleted.

Information Management (IM)

Planning, budgeting, manipulating, and controlling information throughout its lifecycle. (AR 25-1)

Information Technology (IT)

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. Also includes computers, audio visual, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. (AR 25-1)

Information Technology Asset Management

Management of IT assets, including hardware, software, contracts, services and licenses.

Information services

Any service performed in support of information management. Included are automation, visual information, telecommunications, and integrated information, and printing and publication support activities.

Information system

Organized assembly of resources and procedures designed to provide information needed to execute or accomplish a specific task or function. Information system equipment consists of components (e.g., hardware, software, firmware, products, or other items) used to create record, produce, store retrieve, process, transmit, disseminate, present, or display data or information.

Information system component

Hardware, software, firmware, products, procedures, or other items used in the assembly of information systems.

Information system equipment

Equipment that is a configuration of one more information system components used for the creation, recording, production, storage, retrieval, processing, transmission, dissemination, presentation, or display of data or information. Information system equipment is used to perform functions associated with automation, telecommunications, visual information, printing, publishing, and records management in support of the Army's mission.

Initiative

An IM/IT initiative is an effort with a sponsor and budget that has a defined scope with an estimated start date and an end date. Initiatives can be related to improvement efforts or implementation of a new system, technology, process, or service. Initiatives are not mandatory maintenance and repair or operational continuity/sustainment unless those costs were un-forecasted or not part of the initial business case.

Knowledge Management (KM)

An approach to improving organizational outcomes and organizational learning by introducing into an organization a range of specific processes and practices for identifying and capturing knowledge, know-how, expertise and other intellectual capital, and for making such knowledge assets available for transfer and reuse across the organization.

Long-term record

The designation applied to records that have value beyond the business process, such as for historical, lessons learned, or research purposes. This type of record is kept longer than 6 years.

Office Record List (ORL)

A list of the specific record titles and/or numbers describing the records accumulated or generated in an office. The list is prepared within each element where records are accumulated or generated and should be coordinated with the organization or installation records management official.

Official Record

Official records include all documentary materials, regardless of physical form or characteristics, that provide evidentiary accounting for decisions, policies, plans, organizations, functions, procedures, operations, and essential transactions of an organization (as defined in 44 U.S.C. 3301).in 4

Operational Facilities (OPFAC) Allocations

A set of guidelines that define functional elements (i.e., a generic duty positions such as action officer or senior executive, or a place such as a conference room) and apply assignment rules, allocation rules, and IM/IT requirements descriptions corresponding to the functional element. TRADOCs OPFAC guidelines are available on the AKO IT RAD portal.

Public web site

A web site that is accessible from the Internet and uses no positive access control, for example, user authentication or firewalls, to restrict access to the information posted on the web site. Web site is used to also include any network service that gives a persistent presence to information on the Internet, with or without a Hyper Text Transfer Protocol (HTTP) front end (for example, File Transfer Protocol (FTP) site).

Private web site

A web site that screens or challenges users prior to permitting access to the information posted on the site. Private web sites may be connected to an intranet (that is, users are screened from accessing the entire network) or the Internet (that is, users are screened before entry into the specific web site). The term 'web site' also includes any network service that gives a persistent presence to information on the Internet, with or without an HTTP front end (for example, FTP site).

Permanent record

The designation applied to records worthy of permanent retention by the United States, and accessioned into the National Archives until the end of democracy.

Record copy

That copy of a record kept by the agency, office, or element directly responsible for the function to which the record relates that has been identified as the copy to be maintained to document the action taken or business transacted. Record copies of incoming or outgoing communications may be in a variety of forms. These include electronic copy, paper copy, handwritten items, specific media, microforms, etc. IM/IT does not include reading file copies or copies held for convenience or reference.

Sensitive information

Any information the loss, misuse, or unauthorized access to, or modification of, which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (The Privacy Act), but which has not been specifically authorized under criteria established by executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Sensitive information includes information in routine DOD payroll, finance, logistics, and personnel management systems. Examples of sensitive information include, but are not limited to, the following categories:

(1) FOUO - in accordance with [DOD 5400.7-R](#), information that may be withheld from mandatory public disclosure under the FOIA.

(2) Unclassified technical data — Data related to military or dual-use technology that is subject to approval, licenses, or authorization under the Arms Export Control Act and withheld from public disclosure in accordance with DODD 5230.25.

(3) Department of State (DOS) Sensitive but Unclassified (SBU) — Information originating from the DOS that is determined to be SBU under appropriate DOS information security policies.

(4) Foreign Government Information — Information originating from a foreign government that is not classified CONFIDENTIAL or higher but must be protected in accordance with DOD 5200.1-R.

(5) Privacy data — Personal and private information (for example, individual medical information, home address and telephone number, and social security number) as defined in the Privacy Act of 1974. (AR 25-2)

Shareable Content Object Reference Model (SCORM)

An XML-based method for representing course structures. IM/IT enables the reuse of web-based learning content across multiple environments and products.

Short-term record

The designation applied to records that have no value beyond the business process and usually not kept longer than 6 years.

Total program costs

All expenditures for research, development, procurement, installation, and maintenance necessary to field a solution for a stated requirement.

Warfighting requirements

Warfighting requirements are requirements for acquisition category I-IV weapons and materiel systems, automated information systems, IM/IT programs, special access programs, and clothing and individual equipment in direct use by or support of the Army warfighter in training for and conducting operational missions (tactical or other), or connecting that warfighter to the sustaining base. (AR 71-9)

USAREC

ELECTRONIC PUBLISHING SYSTEM

DATE: 27 MARCH 2019
DOCUMENT: USAREC REG 25-1
SECURITY: UNCLASSIFIED DOC
STATUS: EXPEDITED REVISION