

Standard GOV-14 Job Aid

IT OPERATIONS	REFERENCES	GO/NO GO	COMMENTS
14a(2) Institution validates the use of (HQ, TRADOC funded), long distance services.	TR 25-1, 1-6c and TR 25-1, 3-8c(2)e		The purpose is to assure that long distance services that are funded by HQ, TRADOC G-6 are still valid requirements.
RECORDS MGMT, FOIA, & PRIVACY ACT	REFERENCES	GO/NO GO	COMMENTS
14b(1) and 14(b)(2) Ensure the organization has a Records Manager identified and records management, Freedom of Information Act (FOIA), and Privacy Act procedures in place. Ensure the organization coordinates with the TRADOC Records Administrator.	AR 25-1, chap 8; AR 25-400-2, para 1-4e; and DA Pam 25-403, para B-3. AR 25-1, paras 2-15n and 8-5		Duty Appointment Orders. Complete program evaluation questions in DA Pam 25-403, paragraph B-3 at http://www.apd.army.mil/pdffiles/p25_403.pdf . All References listed. TRADOC Records Administrator, Office of the G-6, Information Integration Division.
14b(3) Ensure the records manager and records coordinators are registered in ARIMS to create and propose office record lists. Review the organizations master records management spreadsheet (consists of organization offices/record coordinators/office symbols/UICs/complete mailing addresses).	AR 25-400-2; DA Pam 25-403, para 1-6 (spreadsheets located at RM Portal: https://cac.tkeportal.army.mil/sites/g6/ii/Records_Management/default.aspx		Organization Master Records Management Spreadsheet. ORLs are created by accessing and registering on the web-based Army Records Information Management System (ARIMS) located at: https://www.arims.army.mil/MainPage.aspx . Once the draft ORL is proposed by the records coordinator, an e-mail is sent to the Records Manager requesting approval.

<p>14b(4) Ensure files (hardcopy and electronic) been marked IAW ARIMS and the Privacy Act? Review hard copy files for ARIMS labels and review electronic files, share drives, or share portals for ARIMS file titles. Review location of personnel records to ensure personally identifiable information record labels have reference to Privacy Act system of record notice number and they are secure. For example, office temporary duty travel Privacy Act Number is: T7333DFAS.</p>	<p>The Privacy Act; AR 340-21; AR 380-5; AR 25-400-2, para 6-2 and DA Pam 25-403, paras 3-8 and 3-22</p>		<p>Interview the Records Manager and review where organization records are located (hardcopy and electronic) to see if they have ARIMS labels. Inquire how sensitive records are safeguarded.</p>
<p>14b(5) Ensure the organization adheres to the disposition instructions associated with ARIMS record numbers?</p>	<p>DA Pam 25-403, chaps 4, 7, and 10. See DA Pam 25-403, para 7-5c for SF 135 procedure</p>		<p>Only record numbers listed in the ARIMS Records Retention Schedule – Army (RRS-A) https://www.arims.army.mil/RRSA/Search.aspx are authorized.</p>
			<p>Review keep records. For example, Quotas - Offices other than office having Army-wide responsibility records disposition is “KEN. Event is after next comparable survey or inspection. Keep in CFA until event occurs and then up to 6 years after event, then destroy. Office being inspected, use RN 1c, inspections and surveys.” Are inspection records destroyed 6 years since the next survey/inspection maintained for 6.25 years?</p>
			<p>Review transfer records. For example, office temporary duty travel records disposition is “T6.25. Keep in CFA until no longer needed for conducting business, then retire to RHA/AEA. The RHA/AEA will destroy record when the record is 6.25 years old.” Are TDY records maintained for 6.25 years?</p>
			<p>Review permanent records. For example, School</p>

			<p>reports - Requiring offices performing Army-wide responsibility: Consolidated or summarized reports record disposition is "PERMANENT. TP. Keep in CFA until no longer needed for conducting business, then retire to RHA/AEA. Destroy feeder reports 2 years after data is extracted."</p>
<p align="center">TRADOC IT ACQUISITION MANAGEMENT</p>	<p align="center">REFERENCES</p>	<p align="center">GO/NO GO</p>	<p align="center">COMMENTS</p>
<p>CRITERION: 14.c.1.</p> <p>REQUIRED DOCUMENTS: MIPRs, Contracts / Delivery Orders, and Government Purchase Card (GPC) files for IT hardware, software and services purchases over the last 12-month period. Approved CHES Waivers for non-CHES purchases, and approved CB Exception Memos for non-CB purchases of desktop and notebook computers, plus monitors</p> <p>1. Is the organization using authorized contracts for IT hardware and software purchases or getting an approved Waiver? Specifically for desktop and notebook computers, plus monitors, ss the organization purchasing during the authorized CHES Consolidated Buy periods or getting an approved Exception?</p>	<p>Memorandum, SAIS-GKP, 04 May 2009, subject: Use of Computer Hardware, Enterprise Software and Solutions (CHES), Army Regulation (AR) 25-1, DA PAM 25-1.</p>		<p>(1) Referenced Memorandum, SAIS-GKP, 04 May 2009, subject: Use of Computer Hardware, Enterprise Software and Solutions (CHES) as the Primary Source for Procuring Commercial Information Technology (IT) Hardware and Software, co-signed by Army CIO/G6 and ASA(ALT), Referenced memorandum changes guidance published in Army Regulation (AR) 25-1, and requires the use of CHES managed contracts to include the DOD /Federal SmartBUY Enterprise Software Agreements for the purchase of all Commercial-off-the-Shelf hardware and software regardless of cost. It also clarifies guidance in AR 25-1 on use of CHES managed contracts for IT services as a recommended but not mandatory source. A list of all CHES and DOD ESI Contracts are on the CHES website at https://chess.army.mil/ascp/commerce/index.jsp (Contracts and Agreements, plus Software, links).</p> <p>If your hardware or software requirement is not available on any of these contracts, you must request a Waiver from CHES at https://chess.army.mil/ascp/commerce/ESI/waiver/index.jsp</p>

		<p>(2) All desktop and notebook computers, plus monitors, must be purchased via the Consolidated Buy (CB) process, else a CB Exception Memo must be submitted and approved. Consolidated buy information can be found at https://chess.army.mil/ascp/commerce/consolidatedBuy/index.jsp.</p> <p>(3) If a contractor is purchasing hardware, software or services on your behalf in support of TRADOC missions, the Contracting Officer shall provide your contractor an Authorization Letter which allows them to purchase from these contracts or the government POC must request a Waiver from CHES.</p>
<p>2. Has the organization analyzed and documented it's mission and related work processes before making significant IT investments to support these processes?</p>		<p>AR 25-1, Appendix C, Management Controls Checklist.</p>
<p>CRITERION: 14.c.3.</p> <p>REQUIRED DOCUMENTS: NONE (TRADOC G-6 has a record of all RADs submitted and approved over the last 12-month period).</p> <p>3. Does the organization follow the TRADOC mandated Requirements and Acquisition Decision(RAD) process as outlined in TRADOC Regulation 25-1, Chapter 3 for acquiring new technology?</p>	<p>TR 25-1, Chapter 3, including Change 1.</p>	<p>Using the REQUIRED DOCUMENTS for CRITERION 6.c.1, ensure RAD Approvals have been obtained for all IT hardware, software, and services purchases >\$25K, or for server, server software, or collaboration software purchases regardless of cost.</p>
<p>CRITERION: 14.c.4.</p> <p>REQUIRED DOCUMENTS: NONE (TRADOC G-6 has a record of all APMS items for your organization).</p>	<p>Appendix D, Army IT Portfolio Management Guidance, dated</p>	<p>(1) IT Investments must be entered into APMS if they meet the following criteria: the cost of the investment is >\$25K in any one year of the Future Years Defense Program (FYDP), the investment has</p>

<p>4. Have all IT Investments (systems, networks, databases) and costs associated with these Investments (hardware & software purchases, sustainment costs, IT development and support contracts, etc) been entered into the Army Portfolio Management Solution (APMS) System?</p>	<p>9 March 2008.</p>		<p>undergone or is required to undergo a Certification and Accreditation (C&A), or the IT investment is an Army initiative that has been certified by the Defense Business Management Systems Committee (DBMSC). NOTE 1: The FYDP consists of Prior Year (PY), Current Year (CY), and 6 Budget (future) Years (BY). NOTE 2: you do not need to include applications that are on the Army Gold Master or AKO portals. (2) Using the REQUIRED DOCUMENTS for CRITERION 6.c.1, ensure IT Investments meeting the criteria above have been entered into APMS.</p>
<p>5. Does the organization have a documented process in place for implementing performance measures and reviewing performance of IT systems and contracts on a periodic basis?</p>			<p>Be prepared to show documentation of performance review process.</p>
<p>COLLABORATION TOOLS</p>	<p>REFERENCES</p>	<p>GO/NO GO</p>	<p>COMMENTS</p>
<p>6d(1) Ensure collaboration tools are used in accordance with Army and TRADOC guidance.</p>	<p>TR 25-1, Para 5-2.a</p>		

14d(2) Has the organization identified an Army Knowledge Online (AKO) administrator?	TR 25-1, Para 1-5.f(7)(b)		
14d(3) Has the organization created an AKO Knowledge Center?	TR 25-1, Para 5-3.a(1)		AKO (https://us.army.mil) is the Army's intranet and the preferred collaboration capability. TR 25-1, paragraph 5-3.a(1) requires all organizations listed in TRADOC 10-5 to have a Knowledge Center on AKO and use it for content that must be available to the Army community.
14d(4) Has the organization employed collaboration capabilities that duplicate existing solutions such as AKO, TRADOC Knowledge Environment (TKE) and Battle Command Knowledge System (BCKS)?	TR 25-1, Para 5-2.a		AKO (https://us.army.mil) is the Army's intranet and the preferred collaboration capability. TKE is a TRADOC-hosted portal and is appropriate for development and sharing of internal TRADOC/organizational content. (https://tke.army.mil/default.aspx). BCKS provides a network of structured professional forums (SPF) focused on knowledge transfer and leader development (https://bcks.army.mil).
14d(5) Is content on web sites and portals linked to the authoritative source, rather than copied or duplicated on that site?	TR 25-1, Para 5-3.a(4)(b)		
14d(6) Does PAO approve the release of content prior to its publication on public web sites?	TR 25-1, Para 5-3.a(4)(c)		

INFORMATION ASSURANCE	REFERENCES	GO/NO GO	COMMENTS
14e(1) Ensure the organization has an IASO/IAM identified and on orders.	AR 25-2, Para 3-2		Duty appointment orders should be uploaded to the Army Training Certification and Tracking System (ATCTS) https://atc.us.army.mil/iastar/index.php for viewing.
14e(2) and 14e (3) Ensure all users and IA personnel meet the training and clearance requirements for access to DOD information systems. Users must also sign an Acceptable Use Policy (AUP) acknowledging their understanding of system use policy	AR 25-2, Para 3-3, 4-3, 4-14, and 4-5r; Army's Training and Certification BBP		Verify IA personnel certification status in ATCTS https://atc.us.army.mil/iastar/index.php . Spot check signatures and verify the content of the AUP.
14e(4) Ensure IA personnel receive IAVM notices from the IAVM Community Group.	AR 25-2, Para 4-24.c (1)(d)		IA personnel should receive automatic emails from the Army IAVA mailing list when new IAVAs are published.
14e(5) and 14e (6) Verify the organizations systems the meet the requirements of 6c (4) are registered in APMS. Those systems in APMS requiring DIACAP must have a current Authority to Operate (ATO) or Interim Authority to Operate (IATO). Annual reviews are conducted.	AR 25-1, Para 3-4, DoD 8510.01		Verify this information with TRADOC IA
14e(7) Ensure all applications in use in the organization have a valid (CON)	AR 25-2, Para 4-5b.		The link for the approved CON list is https://www.us.army.mil/suite/doc/17987760

14e(8) Ensure the organization only uses approved IA tools.	AR 25-2, Para 4-20i.		Verify any IA tools against the IA tools list located at https://informationassurance.us.army.mil/ia_tools/AI_AAPL.pdf
14e(9) and 14e(11) Ensure audit servers are used to maintain and review audit logs on mission systems. Ensure high-risk services of mission systems are not used.	AR 25-2, Para 4-5h.		These criterions refer only to mission systems.
14e(10) Ensure IA personnel are familiar with incident procedures	AR 25-2, 4-21 w/TRADOC Supplement 1.		Review the organizations incident reporting procedures and verify that IA personnel know there roll in the process.
14e(12) Ensure users encrypt or digitally sign E-mail messages as required.	Army Digitally Signing Email BBP, AR 25-1 Para 6-4m(7)		Verify that users are familiar with the policy (Encrypt messages that contain sensitive information; Sign messages with active Hyperlinks or attachments)
14e(13) Ensure all Protected Distribution Systems (PDS) are approved.	AR 25-2, Para 6-3.		This criterion is for SIPRNet only. Verify that a PDS approval memorandum is on hand.
14e(14) Ensure the organization has a Continuity of Operations Plan (COOP) in the event of major disruptions and the plan is exercised yearly at a minimum.	AR 25-2, Para 4-5i.		The installation NEC will have the COOP plan for the regular network. The organization should have a COOP for its mission systems with a record of annual test.
14e(15) Ensure hard drives containing sensitive or classified information are purged or destroyed when no longer needed.	Army's Reuse of Computer Hard Drives BBP.		Review the BBP (https://informationassurance.us.army.mil/bbp/BBP_hard_drive_reuse_ver_1%207.pdf) for detailed requirements for destruction, purge, and reuse of hard drives . Verify the method of purging or

			destroying hard drives within the organization.
14e(16) Ensure the organization is familiar with spillage procedures.	AR 25-2, Para 4-16d; and Army's Classified Spillage BBP.		Review the BBP (https://informationassurance.us.army.mil/bbp/classified_spillage.pdf) for detailed requirements for spillage procedures. Verify personnel are familiar with the procedures.
14e(17) Ensure the organizations wireless networks comply with FIPS 140-2 and the Army's Wireless Security Standards BBP.	Army's Wireless Security Standards BBP.		Review the BBP (https://informationassurance.us.army.mil/bbp/BBP_Wireless_Security_Standards_VER_3_0.pdf) for specific requirements for wireless networks.