

Information Management

Information Resources Management Program

For the Commander:

DAVID L. SLOTWINSKI
Colonel, GS
Chief of Staff

Official:

ROGER H. BALABAN
Director, Information Management

History. This UPDATE publishes a new regulation which is effective 31 December 2000.

Summary. This regulation assigns responsibilities, establishes policy and procedures, and provides guidance for the United States Army Recruiting Command Information Resources Management Program.

Contents (Listed by paragraph number)

Chapter 1

General

- Purpose ● 1-1
- References ● 1-2
- Explanation of abbreviations and terms ● 1-3
- Scope ● 1-4
- Policy ● 1-5
- Responsibilities ● 1-6
- Procedures ● 1-7

Chapter 2

Request for IM Support

- Responsibilities ● 2-1
- Procedures ● 2-2
- ITE or non-ITE decisions ● 2-3
- End-user programming ● 2-4

Chapter 3

IT Education

- General ● 3-1
- Training ● 3-2
- Information assurance training ● 3-3

Chapter 4

Microcomputer Software and Hardware

- Government-procured software ● 4-1
- Privately-procured software ● 4-2
- Games ● 4-3
- Working at home ● 4-4
- Software and durable ITE inventory and accountability ● 4-5
- Files responsibilities ● 4-6
- Government-produced software by another Government agency ● 4-7
- Government-procured hardware ● 4-8
- Privately-owned, -leased, -rented, or -borrowed hardware ● 4-9
- Violations ● 4-10

Applicability. This regulation is applicable to all elements of the United States Army Recruiting Command.

Supplementation. Supplementation of this regulation is prohibited.

Proponent and exception authority. The proponent of this regulation is the Director of Information Management. The proponent has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation. Proponent may delegate the approval authority, in writing, to a division chief within the proponent agency in the grade of GS-14.

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.

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 (RCIM-RMP), 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.

RWS ● 4-11

Hardware and software BOI ● 4-12
Hardware and software turn-in and reutilization ● 4-13

Chapter 5

Systems Assurance

- Purpose ● 5-1
- Scope ● 5-2
- Responsibility ● 5-3
- Authority ● 5-4

Chapter 6

Communications

- Telecommunications ● 6-1
- E-mail ● 6-2
- Electronic bulletin boards ● 6-3
- Internet and Intranet ● 6-4

Chapter 7

Audiovisual and Video Teleconferencing Support

- Responsibilities ● 7-1
- Capabilities ● 7-2
- Support scheduling ● 7-3

Chapter 8

Administrative Services

- Administrative Services Branch ● 8-1
- Office automation ● 8-2
- Records management procedures and inspections ● 8-3
- Publications, forms, and printing management ● 8-4

Chapter 9

Systems Documentation

- Purpose ● 9-1
- Scope ● 9-2
- Responsibility ● 9-3

Authority ● 9-4

Chapter 10

Preventive Maintenance and Housekeeping

- Sites ● 10-1
- Cost ● 10-2
- Policy ● 10-3
- Inspections ● 10-4

Chapter 11

Procedures for Preparation and Processing of System Change Requests

- Submission form ● 11-1
- Submission process ● 11-2
- CM Office processing ● 11-3
- Impact analysis ● 11-4
- Approved request ● 11-5
- Documentation ● 11-6
- Development ● 11-7
- Close project ● 11-8
- Implementation ● 11-9

Chapter 12

Systems Support

- General ● 12-1
- SOC ● 12-2
- Help Desk ● 12-3
- CM ● 12-4
- Quality assurance ● 12-5
- Risk management ● 12-6
- Test and evaluation ● 12-7
- Release management ● 12-8
- Data standards ● 12-9

Appendix A. References

Glossary

Chapter 1

General

1-1. Purpose

This regulation assigns responsibilities, establishes policy and procedures, and provides guidance for the United States Army Recruiting Command (USAREC) Information Resources Management Program.

1-2. References

For required and related publications and blank forms see appendix A.

1-3. Explanation of abbreviations and terms

Abbreviations and special terms used in this regulation are explained in the glossary.

1-4. Scope

a. This regulation applies to all elements of USAREC utilizing information technology equipment (ITE) and all elements requesting information technology (IT) support to include, but not limited to:

(1) All actions affecting automated information systems (AIS), whether they are processed at Headquarters, United States Army Recruiting Command (HQ USAREC) or at another Government or commercial activity at the direction or request of HQ USAREC or subordinate elements.

(2) All acquisition of IT services, hardware, software by HQ USAREC or subordinate elements.

(3) All users utilizing USAREC mainframe computers and personal computers (PC).

(4) All proposed contracts or agreements with other Government or commercial activities which involve ITE or IT services.

b. The Director of Information Management serves in two capacities. He is the Director of Information Management for USAREC and he is also the Director of the United States Total Army Personnel Command Information Support Activity - United States Army Recruiting Command (ISA-USAREC).

c. ISA-USAREC is a separate command subordinate to the United States Total Army Personnel Command. ISA-USAREC is under the operational control of the USAREC Commanding General. The Director of ISA-USAREC reports directly to the USAREC Chief of Staff (CofS).

d. All references within this regulation referring to the Information Management Directorate or ISA-USAREC are references to the same organization.

1-5. Policy

a. All requests for information management (IM) support will be submitted through command channels to HQ USAREC (RCIM-RMP-A), Fort Knox, KY 40121-2726. These requests should be sent electronically on USAREC Form 1089 (Requirements Statement) or entered directly into the capability request (CAPR) system via the Intranet by recruiting battalion (Rctg Bn) information management specialists (IMS), recruiting brigade (Rctg Bde) information management officers (IMO), the United States Army Recruiting Support Brigade (RS Bde) IM point of contact, or local HQ USAREC directorate's IM points of contact. Original forms with local approving signatures should be retained (in file number 25-1e) by the submitting organization until electronic signature capability is fielded. Requests from Rctg Bns and their subordinate activities will be submitted through the Rctg Bn IMS and forwarded through the Rctg Bde IMO for further review and recommendation of approval or disapproval. Requests from the RS Bde and their subordinate activities will be submitted through the RS Bde IM point of contact for further review and recommendation of approval or disapproval.

b. ITE and services will generally be provided in accordance with a standard basis of issue (BOI). The BOI prescribes where equipment is to be located. Regardless of whether the ITE is a BOI or special issue, ITE may not be physically moved to a different site without coordination of the primary hand receipt holder (PHRH) and/or property book officer (PBO) and written approval from the Director of Information Management.

c. Privacy Act issues must be coordinated with the unit privacy act coordinator. The Privacy Act requires that whenever personal information is requested from an individual that will become part of a system of records retrieved by reference to the individual's name or other personal identifier, the individual will be furnished a Privacy Act statement. This statement is to ensure that individuals know why this information is being collected so they can make an informed decision on whether or not to furnish it. If questions remain, the unit privacy act coordinator should consult the appropriate judge advocate's office.

1-6. Responsibilities

a. USAREC CofS serves as the chairperson of the USAREC Information Management Support Council (IMSC) and provides guidance to the Director of Information Management.

b. The Director of Information Management is responsible for ensuring that Department of the Army (DA), United States Total Army Personnel Command, and USAREC publications are followed in administering the Information Resources Management (IRM) Program and that IT services are provided to USAREC in the most efficient, economical, and effective manner possible.

c. All commanders, directors of HQ USAREC staff elements, and other supported activities are responsible for the management, security, and proper use of all IT resources under their control. Additionally they must:

(1) Make new information support requirements known to the Information Management Directorate in a timely manner to facilitate budgeting and procurement actions.

(2) Assign, in writing, an individual within their organization to serve as point of contact for IM

matters. A copy will be provided to HQ USAREC (RCIM), Fort Knox, KY 40121-2726. For Rctg Bdes and Rctg Bns, the IM point of contact is the Rctg Bde IMO or Rctg Bn IMS, as applicable. For HQ USAREC staff elements, RS Bde, and other supported activities the IM point of contact should be an individual that possesses knowledge of both the organization's mission and IT, and is usually the organization's designated representative for the Information Management Advisory Working Group (IMAWG).

(3) Ensure that an up-to-date inventory of all ITE within their area of responsibility is maintained in accordance with USAREC Reg 735-3. Formal accountability of ITE ultimately rests with the S4, PBO, or PHRH and it is imperative that all changes, especially serial number changes, be routed through that channel.

(4) Prior to turn-in, coordinate release of any ITE in their area of responsibility with the Information Management Directorate, Resource Management and Plans Division.

(5) Coordinate all IT training with the Director of Information Management in accordance with chapter 3.

(6) Be responsive to periodic requests for IT asset information necessary to allow the Director of Information Management to fulfill management control checks and other command-directed IMA related data calls.

d. The RS Bde commander and Rctg Bde commanders are responsible for providing management control mechanisms for IT in their organization. Through the RS Bde point of contact or the Rctg Bde IMO and the use of the Command Inspection Program, commanders ensure that command standard software and systems are properly utilized and that their command is operating in compliance with the provisions of this regulation and the information architecture.

e. Rctg Bde IMO and the RS Bde point of contact will:

(1) Administer the IRM Program for their organization and subordinate activities. Provide guidance, train, and assist the Rctg Bn IMS in the performance of his or her duties.

(2) Provide management and oversight of the IRM by conducting command inspections and training in the IT disciplines.

(3) Review and provide recommendations on requests for IT services that are not included in the standard BOI.

(4) Represent the Rctg Bde or the RS Bde, as applicable, in the development of IRM plans.

(5) Assist in identification of the need for IT support such as new software, hardware, or other functional support.

(6) Function as the Rctg Bde information assurance manager (IAM). This does not apply to the RS Bde point of contact. The Rctg Bde IAM will meet the Director of Information Systems for Command, Control, Communications, and Computers (DISC4) requirements for certification.

f. Rctg Bn commanders are responsible for carrying out their portion of IRM which includes management of all IT resources in the Rctg

Bn. Through their Rctg Bn IMS and the use of semiannual reviews of their command IRM Program, commanders ensure that command standard software and systems are properly utilized and that their command is operating in compliance with the provisions of this regulation and the USAREC information architecture.

g. Rctg Bn IMS will:

(1) Administer the IRM Program for the Rctg Bn and subordinate activities.

(2) Provide management and oversight of the IT by conducting reviews and training. Assist in training recruiter training noncommissioned officers to support the Army Recruiting Information Support System (ARISS) as necessary.

(3) Represent the Rctg Bn in the development of IT plans.

(4) Assist the Rctg Bn in identification of the need for IT support such as new software, hardware, or other functional support that is not included in the standard BOI.

(5) Function as the Rctg Bn information assurance officer (IAO) unless the Rctg Bn commander specifically appoints another individual. The Rctg Bn IAO will meet the DISC4's requirements for certification.

h. All users of IT resources will operate in accordance with AR 380-19, that is:

(1) Will safeguard their user identification (ID) and passwords at the For Official Use Only (FOUO) level.

(2) Ensure Government IT resources are used only for valid job requirements or as specifically authorized by competent authority (see para 4-8).

(3) Ensure that hardware and software is secured.

(4) Report security violations to their IAO and/or IAM.

(5) Will use only command authorized software.

i. The PBO or PRRH is responsible for recording and/or hand-receipting all ITE and software in accordance with USAREC Reg 735-3 and the policy on software accountability in paragraph 4-5.

j. Directors and the RS Bde commander will appoint, in writing, a local information assurance officer to act as the primary point of contact for all information assurance matters within their areas. These individuals will not require the DISC4's certification.

1-7. Procedures

a. All requests for IT support will be evaluated by the Information Management Directorate against current capabilities and capacities and reviewed for scope of effort, potential costs, and information assurance compliance. Alternate sources (external to the Information Management Directorate) will be recommended when required. All emergency and routine requests for IT assets will be requested electronically using USAREC Form 1089. An IT asset is defined as any product and/or service for which the Director of Information Management has the authority and/or responsibility to provide to the command. IT assets include Federal information processing resources such as hardware, software, and support services. The requests will be

acknowledged by the Information Management Directorate and then reviewed for scope of effort and potential costs. The requests will be presented to the IMAWG for approval or disapproval and, if approved, initial funding prioritization. The IMAWG will meet as needed or up to four times per year and is comprised of IM points of contact from each of the HQ USAREC directorates and the RS Bde, and Rctg Bdes. The IMAWG will recommend the priority of the pending requests and a report of the proceedings will be furnished to the IMSC.

b. Emergency requests for IT support will be electronically submitted to the Director of Information Management for approval or disapproval using USAREC Form 1089. The Director of Information Management may approve up to \$5,000 out of cycle, otherwise the item must be forwarded to the CofS for approval. If there are disputes, the final decision is reserved for the USAREC CofS.

c. The USAREC IMSC will convene as required to review IT requirements and establish top level prioritization and direction. HQ USAREC directors and Rctg Bde commanders will be primary members of the council and the USAREC CofS will serve as chairperson. The Director of Information Management will then execute against the established command priorities.

d. The USAREC Configuration Control Board (CCB) meets at least quarterly and establishes a cooperative environment for providing configuration management (CM) guidance regarding the development, acquisition, fielding, installation, and/or modification of USAREC information systems. The USAREC Commanding General is president of the CCB and the board will be chaired by the USAREC CofS. HQ USAREC directors are the process owners and will be primary or voting members of this board.

e. In all procurement cases, where the identity of a piece of equipment as ITE or non-ITE is in question, a determination will be obtained by the Director of Information Management before any procurement or commitment to procure is made.

f. All data files are the property of the functional proponent whose permission must be obtained prior to file use. Intranet web page content is the responsibility of the content owner and/or proponent.

g. If distributed with the information system, master software diskettes and/or compact disks will be secured so as to preclude loss or theft. Any systems and/or software manuals and original media must be maintained and transferred with the system when it is moved, reutilized, or turned in.

h. All ITE and related software will be accounted for in accordance with AR 710-2, USAREC Reg 735-3, and paragraph 4-5, this regulation. This requires, at a minimum, a log with serial number of the information system and the type of software loaded on that system, and allows for local hand receipt of software disks and/or compact disks to ensure accountability.

i. Requests for software modifications, including those related to data elements, shall be submitted through the appropriate HQ USAREC

directorates (process owner) who, after reviewing and approving the modification, shall prepare an HQ USAREC Form 1913 (System Change Request) and forward it to Information Management Directorate, CM Office, for further processing. All data element standards will be implemented based on the ARISS data dictionary, which is based on DOD 8320.1-M-1. Any request for data element changes shall be forwarded to Information Management Directorate, CM Office, using an HQ USAREC Form 1913.

Chapter 2

Request for IM Support

2-1. Responsibilities

a. Director of Information Management will:

(1) Ensure that receipt of an electronically submitted USAREC Form 1089 (see fig 2-1) is acknowledged.

(2) Ensure that a stored record of the USAREC Form 1089 is maintained, a CAPR (tracking) number assigned, and a working copy is processed to the Chief of Resource Management and Plans Division the same day it is processed into the IM CAPR database.

(3) Maintain an active database for all USAREC Forms 1089 submitted throughout the command by fiscal year (FY).

(4) Provide the requester with status, by CAPR number, upon request, and upon conversion of the IM CAPR database from a local area network (LAN) application to an Intranet application, provide the requester with an on-line capability of obtaining status.

(5) Upon assignment of an analyst to serve as action officer, provide the requester with the name and telephone number of the action officer and modify the IM CAPR database to reflect the action officer assignment.

(6) Determine the potential impact of new IT initiatives or business practice changes which leverage IT in relation to total systems requirements, priorities, capabilities, resources, and security.

(7) Determine the development and sustaining resource costs associated with satisfying the command's IT requirements and submit appropriate budget documents to meet requirements.

(8) Approve or disapprove requests for IT assets based upon findings derived during the review process. In case of conflict the USAREC CofS will make the final decision. In case of approval, forward the approved action to the Director of Resource Management and the RS Bde for tables of distribution and allowances documentation, if applicable, prior to initiating procurement action.

(9) Return disapproved requests to the requester, with supporting rationale.

(10) Obtain IT assets through external sources (contract) in accordance with AR 25-1 if requirement cannot be satisfied by in-house personnel within the Information Management Directorate.

b. Information Management Directorate, CAPR Office, will:

(1) Acknowledge receipt of USAREC Forms 1089 and provide requesters with the assigned CAPR numbers for tracking purposes.

(2) Review USAREC Forms 1089 to prevent duplication of existing USAREC Forms 1089.

(3) Assign tracking numbers (CAPR numbers) using the format: FY-DIR-XXXX. Where FY represents the fiscal year, DIR represents the three-letter abbreviation of the Directorate or Rctg Bde, and XXXX is a sequential serial number which restarts at the beginning of each FY.

(4) Forward USAREC Forms 1089 to the Chief of Resource Management and Plans Division for disposition (i.e., forward requests for out of cycle to the Director of Information Management (not to exceed \$5,000) or to the CoS (all requests for out of cycle which exceed \$5,000) for approval, and/or process the action through the technical review board and IMAWG).

c. Requesting agents for directorates and units will:

(1) Electronically submit all requests for IT assets to include Federal information processing resources (USAREC Form 1089) to the Information Management Directorate, CAPR Office, using USAREC's e-mail system following the instructions in table 2-1. Attachments

may be required for some types of requests, especially those with equipment lists. Field elements will also use this procedure, but will route their requests through the Rctg Bde IMO for review, approval, and forwarding as necessary.

(2) Rank order by category all outstanding USAREC Forms 1089 and submit the priority lists to the IMAWG for inclusion in the work load planning sessions.

(3) Designate a functional subject matter expert (SME) to be the representative of the directorate or office (the functional proponent and the "owner" of the project). The SME is responsible to initiate each project by generating an HQ USAREC Form 1913 or USAREC Form 1089 as appropriate. The SME provides detailed requirements specifications and all specific functional details of the project with emphasis on the execution of user reviews. The SME presents requirements at change control review boards (CCRB) and, as necessary, defends requirements at CCB. The SME actively participates throughout the life of the project to provide further direction as necessary.

(4) Request an ITE or non-ITE decision from the Director of Information Management on any equipment where the classification is not clear prior to starting any procurement action.

(5) Inform the Director of Information Management, in writing, whenever currently maintained data or programs are determined to be no longer needed.

2-2. Procedures

a. USAREC Form 1089 submission. All requests to procure previously approved commercial off-the-shelf software (e.g., MS-Office) shall be submitted using USAREC Form 1089.

b. HQ USAREC Form 1913 submission (see fig 2-2). All requests for changes to existing software applications and requests for new in-house software application development will be submitted by the functional proponent using an HQ USAREC Form 1913 to the Information Management Directorate, CM Office.

2-3. ITE or non-ITE decisions

Requests for determination as to whether a particular piece of equipment is ITE or not will be forwarded to the Information Management Directorate with all technical information available on the equipment. The requester will be notified of the determination by the Information Management Directorate.

**Table 2-1
Instructions for completing USAREC Form 1089**

Block	Title	Remarks
1	REQUEST #	HQ USAREC only. This block contains HQ USAREC's sequentially assigned tracking number which is used to track the request from creation to completion.
2	DIRECTORATE #	Optional. Rctg Bde IMO or RS Bde or HQ USAREC directorate IM points of contact can enter their own number for internal tracking purposes.
3	REQUEST DATE	Automatic. The date is automatically entered by the system upon creation.
*4	DESCRIPTION	Enter a short description of the requirement. Be as generic as possible (i.e., Desktop PC and LaserJet Printer).
*5	REQUIREMENT	Describe the requirement in terms of what is to be accomplished. For example: ITE for Mission Branch to create documentation pertaining to command strength. Explain, if possible, what is needed, by whom, where it will be used, what it will be used with, how it will be used, and when it is needed. If specific make and model hardware and/or software, or a service provided by only a single source is required, explain why no other product or service will satisfy the requirement. If an "Equal" product will satisfy the requirement, specify the salient characteristics of the product, Intel processor, minimum 200 Mhz, 1GB hard drive, 32MB memory, etc. Explain, if possible, what other hardware and software the requested product must interface with and/or be compatible with.
*6	JUSTIFICATION	Explain why the requested items or services are needed to meet the mission or enhance operations, or why the mission cannot be satisfied with existing resources, or what will happen if the request is disapproved.
7	HQ PROPONENT & RECOMMENDATION	Information Management Directorate only. For Rctg Bde and/or Rctg Bn requirements only. Information Management Directorate enters the headquarters proponent's name and recommendations.
8	IM POC & RECOMMENDATION	Information Management Directorate only. Information Management Directorate enters the analyst's name and recommendations.
*9	ITEMS REQUIRED	Enter the items required. Use generic items if necessary (i.e., Desktop PC). Enter the quantity needed and unit cost. The system will calculate the subtotal and total.

Table 2-1
Instruction for completing USAREC Form 1089--continued

Block	Title	Remarks
*10	REQUESTING AUTHORITY	Enter the name, rank or grade, title, and telephone number of the director, special staff section chief, RS Bde commander, or Rctg Bde commander. This block is to be signed by the requesting authority and dated and retained at the requester's office for audit purposes. USAREC Form 1089 is to be electronically transmitted to the Information Management Directorate, CAPR Office.
*11	REQUESTING AGENCY IMO/POC	Enter the name, rank or grade, title, and telephone number of the requesting agency IM point of contact. This is the directorate, special staff section, or RS Bde office IM point of contact, or the Rctg Bde IMO.
*12	PURCHASE TYPE	A drop-down menu will provide the acceptable choices for this entry. They include normal or out of cycle. Normal requests are processed through the next technical review board and IMAWG. Out-of-cycle requests are for requests that need to be processed immediately. The Director of Information Management can approve out-of-cycle requests up to \$5,000. All out-of-cycle requests that exceed \$5,000 must be approved by the USAREC CofS.
*13	ACTION PENDING	A drop-down menu will provide the acceptable choices for this entry.
*14	APPROVAL AUTH	A drop-down menu will provide the acceptable choices for this entry.
15	ACTION OFFICE	Information Management Directorate only. Information Management Directorate's assignment of action office.
16	ACTION OFFICER	Information Management Directorate only. Information Management Directorate's assignment of action officer.
*17	PRIORITY #	Enter 1, 2, or 3 with priority 1 receiving the highest priority processing; priority 2 receiving higher than normal, but not as high as priority 1; and priority 3 as normal processing.
18	ADDITIONAL INFORMATION	Optional. Use this block to expand on other blocks or to provide additional information not provided elsewhere.
*19	SUGGESTED VENDOR	Enter the suggested vendor, if known. Include the address and points of contact with telephone numbers.
*20	SHIP TO PBO/SUPPLY FOR DISTRIBUTION TO	Enter the PBO or PHRH the requested items are to be shipped to and accounted for. Include the point of contact and telephone number.
*21	DELIVERY DATE	Enter the required delivery date.

* Indicates fields that must be provided by requester.

2-4. End-user programming

a. End-user programming on USAREC multi-user computers is restricted to only headquarters personnel who have been authorized to do so. No field users are authorized to write, compile, or use programs that have not been approved by the Information Management Directorate for directorate requirements.

b. End-user programming on microcomputers is restricted to those applications written using standard USAREC tools, specifically the Microsoft Office Professional which can be used only in the office where written, unless approval is obtained from the Director of Information Management.

c. Distribution of a user-written application to other offices may only be authorized in accordance with the following procedures:

(1) Submit a memorandum through the chain of command to the Director of Information Management, subject: Request to Distribute User Written Software. At enclosure 1 provide a de-

scription of the program to include printouts of reports or forms and specify the purpose of the program. At enclosure 2 provide documented source code. At enclosure 3 provide a diskette with the program in executable form. At enclosure 4 provide documentation (see chap 9).

(2) The Director of Information Management will determine who the functional proponent(s) should be and forward copies of the package to them.

(3) The functional proponent will determine if the application should be distributed as is, modified, or not distributed. The functional proponent will notify both the Information Management Directorate and the original requester of the decision.

(4) If it is determined that the application will be distributed, the functional proponent will request that Information Management Directorate commence an evaluation of the product's technical and security implications and normal processing, as described in this chapter, will continue.

Chapter 3
IT Education

3-1. General

To ensure enforcement of command standard software and use of command systems, IMA training will be coordinated with the Director of Information Management at least 30 days prior to any scheduling and training being effected.

a. The necessary enrollment procedures will be performed by the requester's office.

b. DD Form 1556 (Request, Authorization, Agreement, Certification of Training, and Reimbursement), if required, will be prepared by the requesting office. The Information Management Directorate budget officer's signature for expenditure of funds is required for training funded by the Information Management Directorate.

c. Preparation of DD Form 1610 (Request and Authorization for TDY Travel of DOD Personnel) and travel arrangements, if necessary, will be done by the requester's office.

3-2. Training

a. Limited hands-on training of end users on IM microcomputers and software is provided by the Information Management Directorate.

b. Information Management Directorate and Rctg Bde IMO have interactive and videotape training support for command standard software (i.e., Windows NT, Microsoft Office, Word, Excel, PowerPoint, etc.). Additional tutorial and on-line training is available via the USAREC Intranet.

c. Contractual training on ITE is the responsibility of the appointed contracting officer representative.

d. Software packages written specifically for functional proponents will be the responsibility of the functional proponent. Information Management Directorate will review and approve users manuals, training materials, etc., prior to implementation of training.

e. Recruiting Operations Directorate, Training Division, manages and conducts training to users on operations support software (ARISS recruiter workstation (RWS)).

f. The single IT point of contact for an agency will be the coordinator for all IT training requirements. At HQ USAREC level the IT point of contact is usually the director's designated representative for the IMAWG. At RS Bde level the IT point of contact for all IT training is usually the commander's designated representative for the IMAWG. The Rctg Bde IMO will coordinate Rctg Bde IT training requirements with the Information Management Directorate. The Rctg Bn IMS will coordinate Rctg Bn training requirements through the Rctg Bde IMO.

3-3. Information assurance training

a. The USAREC information assurance program manager will maintain a list of currently available courses leading to the certification of all USAREC information assurance personnel.

b. As soon as possible after appointment all IAM will complete the U.S. Army Information Assurance Manager Course.

c. As soon as possible after appointment all IAO will complete the U.S. Army Information Assurance Officer Course.

d. As soon as possible after assuming the duties of a system administrator (SA) the individual will complete the SA certification courses required by DISC4.

e. SA will be responsible for developing system specific functional user training.

f. IAO will be responsible for developing system specific end user security training and procedures.

Chapter 4

Microcomputer Software and Hardware

4-1. Government-procured software

Government-procured software is only for use on Government-owned or Government-operated hardware. Licensing agreements will describe USAREC's responsibilities for use of this software. If software is loaded on a particular

computer it cannot be used on another system unless it has been uninstalled from the previous computer. Loading software to more than one computer at a time, unless specified by the copyright holder, in writing, is a copyright violation. A copyright violation is a violation of Federal law and carries civil criminal penalties. Failure by any USAREC personnel to comply with the provisions of this paragraph and paragraphs 4-2, 4-3, 4-4, 4-8, and 4-10 may subject soldiers to disciplinary actions under the Uniform Code of Military Justice (UCMJ) and civilian employees to disciplinary or adverse actions under Federal law and regulations.

4-2. Privately-procured software

Privately-procured (purchased, leased, rented, or borrowed without use of Government funds) software will not be used on Government equipment without testing, evaluation, and approval of the Director of Information Management. If an individual has privately-procured software that they feel will help optimize their productivity, they should submit their requirements to the Information Management Directorate for consideration of approval.

4-3. Games

Use of computer games is not authorized on any USAREC mission support ITE.

4-4. Working at home

AR 25-1 contains the Army policy on approval to use employee-owned IT hardware and/or software to process Army-related information at locations other than the Government work site.

a. The use of employee-owned IT hardware and/or software to process Army-related work away from the Government work site must be approved by the Director of Information Management.

b. The products of Army-related work are the property of the U.S. Government regardless of the ownership of the IT hardware and/or software.

c. Government-owned software may be used at home only under the following conditions:

(1) The local commander is responsible for ensuring that no software licensing violations occur.

(2) The user must agree to sign a statement:
(a) Releasing the Government from liability in case of theft, damage, or malfunction.

(b) Acknowledging that the user is responsible for removing all USAREC-owned software from the employee-owned system when it is no longer required or the individual has a permanent change of station or expiration term of service.

(c) When removed, certifying that all Government-owned software and data has been removed from the employee-owned computer.

d. Classified information will not be processed on employee-owned ITE.

e. Only Government-owned hardware will be used to access USAREC automated systems from off site.

f. If approved for use, employee-owned computers must comply with all provisions of AR 380-19, including maintaining current antivirus software on the system. The command standard antivirus and periodic updates may be obtained from their IAO.

4-5. Software and durable ITE inventory and accountability

a. ITE such as external modems, external drives (3 1/2-inch floppy, zip, jazz, superdisk, etc.), PCMCIA (PC card) modems, LAN cards, etc., and manuals valued at under \$300, are designated as durable property. Durable ITE does not require formal property book accountability; however ITE will be managed and accounted for by the PHRH or IM point of contact through normal hand receipt procedures in accordance with AR 710-2 and USAREC Reg 735-3. In addition to signing for accountable items on a local hand receipt to the PHRH, an inventory and log of authorized software and durable ITE will be maintained with the PC and master local hand receipt. As a minimum, the log will contain the model and serial number of the PC on or in to which the item(s) was installed, then such information as the description, manufacturer, model, and actual or locally assigned serial numbers of the durable ITE. The log and all manuals will be maintained with the main central processing unit for the life cycle of the hardware and need only be changed when durable or accountable items are changed out or deleted. The local hand receipt and log will be signed and the original copy of the log will be attached to the PHRH's copy of the local hand receipt.

b. Copyrighted and/or proprietary software does not require formal property book accountability, however, such software will be managed and accounted for by the primary IM point of contact (IMO at Rctg Bde, IMS at Rctg Bn) through an inventory and log of authorized software to be maintained with the PC and primary IM point of contact. As a minimum, the log will contain the model and serial number of the PC in or on to which the software was installed, then such information as the description, manufacturer, model, and actual or locally assigned serial numbers of any other software. Commercial software or the standard baseline for office automation does not require a locally produced or actual serial number. The serial number entry for these six items on the log of software of durable ITE will reflect site-enterprise licenses. The log will be maintained with the main central processing unit for the life cycle of the hardware or software and need only be changed when durable or accountable items are changed out or deleted. The original copy of the log will be signed by the user acknowledging that the software is not authorized to be copied to any other machine.

4-6. Files responsibilities

a. Each individual is responsible for the files they create or use on a microcomputer and is

also responsible for their transfer or removal when the microcomputer is reassigned or turned in. Each user is also responsible for the original documentation, program, and data disks or compact disks assigned to their microcomputer and must return these items with the microcomputer.

b. A standard, managed baseline and common operating environment and specific software version descriptions (SVD) are established for all computers in the command. Under no circumstances will unauthorized software or a change to the software or hardware configuration be accomplished without authorization. Copies of the common operating environment and SVD can be obtained from the Information Management Directorate, CM Office.

4-7. Government-produced software by another Government agency

Some software produced by other Government agencies is for the intended use of Government agencies; therefore, no copyright infringement exists. However, the Information Management Directorate must approve the use of this software on any USAREC equipment. No such software will be used without Information Management Directorate's approval. If you feel such software is necessary to perform your duties, a formal request with full justification must be submitted to HQ USAREC (RCIM-CM), Fort Knox, KY 40121-2726, for consideration.

4-8. Government-procured hardware

a. Government-owned or Government-leased resources are furnished to employees for the conduct of official Government business, and are only to be used for such official business and for other properly authorized purposes.

b. Although more detailed guidance is available in DOD 5500.7-R, chapter 2, the guidance has been expanded to permit some limited use of Government resources, other than personnel, for personal purposes. Such uses are limited to the following:

(1) The use must not adversely affect the performance of official duties by the employee or the employee's organization and must be properly authorized by competent authority (i.e., the first supervisor who is a commissioned officer or a civilian above GS-11 in the chain of command or supervision).

(2) The use must serve legitimate purposes such as telephonic or e-mail communications most reasonably made from your normal workplace (as opposed to taking the employee away from the work location) or supporting volunteer services for the community, enhancing the professional skills of the employee, or assisting in job search for employee in response to Government downsizing.

(3) The use must be of reasonable duration and frequency and made only during the employee's personal time such as before or after duty hours or during lunch or other authorized breaks.

(4) The use must be compatible with public service and must not reflect adversely on the

Government. Prohibited uses include commercial activities, unofficial advertising, soliciting or selling (except on authorized bulletin boards), and uses that are in violation of a statute or regulation.

(5) The use must not create a significant additional cost, in terms of funds and/or work load, to the Government.

(6) The use must not deny IT services to any other Government employee accomplishing assigned missions (telephone lines, limited Internet access, etc.).

c. The rules and regulations governing the use of Government resources are punitive. Failure to abide by their clear guidance may subject members of the command (whether military or civilian) to disciplinary and/or adverse actions. The following areas are direct guidance on avoiding inappropriate use of Government resources:

(1) Absolutely no attempts to find, view, obtain, or distribute pornography.

(2) No e-mailing of chain, group, or mass-distribution letters or messages, especially those that could be perceived by recipients as having official Army and/or USAREC sanction, or would reflect adversely on the Army, or would appear to be incompatible with public service.

(3) No advertising, soliciting, or selling for a private business or as an agent of a commercial business using Government IT systems. Personal items may be solicited or sold only on authorized bulletin boards.

(4) No use of Government-procured software outside the manufacturer's license.

(5) No use of personal software on Government computers without Information Management Directorate's authorization.

(6) No use of personal computer or hardware in the place of duty to conduct official business.

(7) No use of computer games on USAREC automation equipment.

(8) No use of personal homepages or personal Internet accounts on Government IT systems.

(9) No use of Government equipment to engage in any gambling activity.

(10) No use of Government equipment to pass jokes, cartoons, or other inappropriate materials.

4-9. Privately-owned, -leased, -rented, or -borrowed hardware

Computers and peripherals that are not Government-owned or Government-leased will not be used by individuals in their place of duty. If a microcomputer, or a component thereof, is required to perform your official duties your requirements with full justification should be submitted to the Information Management Directorate for consideration.

4-10. Violations

Any violation of information assurance security, to include unauthorized copying of copyrighted software, must be reported as prescribed in AR 380-19. The individual will immediately report the suspected violation to the appropriate IAO. The

IAO will determine if a reportable violation has occurred. The IAO will inform the IAM of the suspected violation and any actions taken. If the situation warrants further action, the information assurance program manager will be apprised and that individual will make the proper notifications.

4-11. RWS

a. All policies for PC and terminals contained in this regulation apply fully to the ARISS RWS laptop.

b. USAREC will maintain replacement ARISS RWS. These systems and components will only be used to replace stolen and significantly damaged units in the field. Faulty, but repairable ARISS RWS, are maintained through a maintenance program defined in the ARISS RWS Logistics Support Plan. Recruiting station (RS) equipment will not be diverted from its intended use or permanently placed in any other operational capacity without the express written consent of the Director of Information Management or his or her designated responsible agent.

c. The configuration of the RWS will be centrally managed and shall not be modified by the field unless directed by HQ USAREC.

d. Any laptop or portable computer, including the ARISS laptops (RWS), issued to a recruiter is considered personal arms and equipment as defined by AR 735-5. If it is lost, a recruiter may be assessed the full value of the laptop. Each recruiter should exercise good judgment and common sense when transporting and storing the ARISS laptop. Each incident of loss will be evaluated on a case-by-case basis to determine personal liability. General guidelines for security of the ARISS laptop are as follows:

(1) USAREC Label 23 (Property of the U.S. Army) shall be placed in the lower left corner of the top of the laptop when the laptop screen is in the closed position. Commanders will be responsible for ensuring this label is affixed to each command-owned laptop. USAREC Label 23 may also be used on other command-owned ITE such as desktops, monitors, scanners, etc.

(2) Keep the laptop in your possession whenever possible. When this is not possible:

(a) Do not leave the laptop in plain view and unattended in an RS, office, Government-owned vehicle (GOV), or a privately-owned vehicle (POV).

(b) When storing the laptop in your office or RS, ensure that the storage location (desk, cabinet, etc.,) is sturdy and locked. When storing in personal quarters be cognizant of the risk of theft or environmental damage.

(c) If the recruiting facility is situated in a high-crime area, increased security awareness is necessary.

(3) When traveling and staying in a motel or hotel and you cannot reasonably take the laptop with you when you go out of your room, you must consider the following options:

(a) Secure the laptop with another person from the command who willingly assumes personal responsibility.

(b) Secure the laptop in your GOV or POV for short periods of time if environmental or security considerations allow.

(c) Temporarily secure the laptop with the lodging's security office and obtain a specific receipt.

(d) If you must leave your laptop in your room, make every attempt to store it out of sight and as secure as possible.

(4) If no other more secure options exist and you must store your laptop temporarily in a GOV or POV, consider the following factors:

(a) The laptop's visibility.

(b) The known crime rate of a particular city or area.

(c) When hidden from view or stored in a vehicle's trunk pay close attention to weather conditions. Extreme weather conditions, such as temperatures above 95 degrees or less than 41 degrees Fahrenheit can damage laptops. Further, heavy rainfall and a leaking trunk may cause water damage.

(5) Airports create additional security hazards. Laptops should never be left unattended in airports. Do not check the laptop as baggage.

4-12. Hardware and software BOI

The current microcomputer hardware and software BOI for Rctg Bdes, Army Medical Department detachments, Rctg Bns, and other locations including the approved Marketing Cell Basis of Issue Plan and the Advertising and Public Affairs Target Architecture, has been posted to the standard office configuration web page under the Information Management Directorate on the USAREC Intranet. Variations require written authorization from the Director of Information Management.

4-13. Hardware and software turn-in and reutilization

IM personnel, at all levels, have a responsibility to assist their commander in managing automation assets. This responsibility should include needs versus wants, assessments, and life cycle replacement considerations. In an effort to avoid waste, fraud, and abuse, all organizations in USAREC are required to report all excess hardware and software for turn-in, destruction, or reutilization. Excess ITE is any hardware or software currently not in use because it has been upgraded, replaced, or is unserviceable. While the commander is ultimately responsible, the user's first step in the redistribution is the IM point of contact. The IM point of contact is responsible for coordinating with the proper IM representative. The Rctg Bn IMS is responsible for coordinating with the Rctg Bde IMO and the Rctg Bde IMO is responsible for keeping HQ USAREC, Information Management Directorate, up-to-date to ensure changes are in accordance with the IRM Program. Finally, all movement of property must be coordinated with the appropriate supply and property accountability personnel.

a. User's procedures for handling excess ITE.

(1) Hardware.

(a) Send memorandum, e-mail preferred, to the organization's IM point of contact for disposition.

(b) You will be provided disposition instructions to complete and notified whether your system is to be redistributed within your area of operation or you will be instructed to turn in your system to supply for outside redistribution. If the equipment is to be turned in, notify the Rctg Bde IMO or Rctg Bn IMS to have the automation equipment certified by an authorized IM representative. At HQ USAREC contact the Service Oversight Center (SOC) and request a ticket be created for equipment certification. The Information Management Directorate (Help Desk personnel) must certify the equipment before the equipment will be accepted for turn-in.

(2) Software. Turn in all excess or old software to the IM point of contact. If original software disks or compact disks and documentation is available they should move with the system. Every system should have a legal copy of its operating system. The disks and documentation, if present, may be stored by the IM point of contact, hand receipt holder, or supply personnel, but every computer must have a unique matching set of software assigned to it.

b. IM procedures for handling excess ITE. Each organization will identify, in writing, an individual within their organization to serve as point of contact for IM matters. For Rctg Bdes and Rctg Bns, the IM point of contact is your or Rctg Bde IMO or Rctg Bn IMS, as applicable. For HQ USAREC staff elements and other supported activities, the IM point of contact should be an individual that possesses knowledge of both the organization's mission and IT, and is usually the organization's designated representative for the IMAWG.

(1) Maintain an internal information systems plan, including priority of fill information, on who has what equipment, and what is needed for each authorized position. Be aware that there are higher level redistribution plans for ITE such as when ITE has been replaced or deemed to be no longer needed. This also applies to windfall excess computers found outside of USAREC. Keep HQ USAREC, Information Management Directorate, informed by sending an e-mail when planning redistribution of automation assets. After completing a transaction, be sure to forward an electronic copy to HQ USAREC (RCIM-RMP-A) so that the maintenance contracts can be properly managed.

(2) Upon receipt of new equipment or notification by the user of excess, use your plan to determine if your organization needs the equipment or software. Unless otherwise directed, redistribute internally. If your organization doesn't need the equipment or software, pass the information to the next level.

(3) Notify the hand receipt holder if the equipment or software is to be turned in or hand receipted to another hand receipt holder within the organization. If the equipment is to be redistributed within the organization, assist supply, when-

ever possible, with the coordination of the appropriate hand receipt holders to effect the transaction.

(4) If the Rctg Bde or HQ USAREC does not need the equipment or software, the Rctg Bde IMO will be authorized to have the hardware or software so designated in the Defense Information Technology Management System (DITMS) for Department of Defense (DOD) wide redistribution. This should be completed by supply personnel; however, entering information into DITMS is not restricted to supply personnel. The IM point of contact and supply personnel will complete the transaction after receiving the disposition from DITMS.

(5) All fixed disks on the ITE will be cleared in accordance with AR 380-19 by degaussing or using WipeInfo or some other DA-approved software. The Information Management Directorate, Information Assurance Office, will make software available to complete this action.

(6) If the software is unserviceable and no negligence is involved, follow the instructions below for software destruction. If the user was negligent in his or her responsibilities to safeguard the software, logistics personnel will initiate appropriate statement of charges or report of survey and then the IM point of contact should destroy the software. Software is destroyed by tearing apart the manuals and recycling the paper products and cutting up or mutilating the disks or media. High density diskettes may be recycled by removing the label and reformatting or degaussing the disks. Destruction is complete when the user receives a memorandum from the IM point of contact, signed by both the IM point of contact and the user stating the name of the software, serial number of the software (if applicable), and when it was destroyed.

(a) All incomplete (missing one or more disks or missing documentation) current software packages (see BOI) should be destroyed as above after the necessary supply and accountability actions have been completed.

(b) All obsolete software packages should be destroyed as above.

(6) If a hardware item is unserviceable, turn it in to the PBO with a memorandum certifying that the item is unserviceable or uneconomical to repair. Or if disposing of hardware locally coordinate with the PBO before taking certified systems to the Defense Reutilization Management Office (DRMO).

(7) Joint Optical Information Network computers must be turned in for disposal. They are no longer useful and are not maintained. Joint Optical Information Network systems can be turned in like any hardware item at the lowest level possible. Since these units are obsolete and can only be used for USAREC purposes, a memorandum exempting these systems from SF 120 (Report of Excess Personal Property) requirements has been issued to all Rctg Bns. In addition, the federal stock number places these units in a training aid category.

c. PBO.

(1) The PBO is solely responsible for ensuring all ITE is entered into the DITMS inventory upon receipt into the command and upon final disposition.

(2) The PBO will process requests for excess ITE on a first-come-first-served basis. The PBO is responsible for releasing ITE by either transferring the equipment to the gaining unit, releasing the equipment to an educational organization enrolled in Computers for Learning, or turning the equipment in to the DRMO for disposal.

(3) If the IM point of contact certifies the ITE as unserviceable or obsolete, the PBO will fill out a DD Form 1348-1A (Issue Release/Receipt Document) and coordinate with the DRMO to deliver the items to the property disposal office storage facility for destruction, auction, or scrap.

d. DITMS is a three-tier, web-based application system supporting the Defense Automation Resources Management Program of the Chief Information Officer. DITMS keeps track of ITE from the time it is recorded as inventory to the time it is reported as excess and becomes available for redistribution. Each Rctg Bde and Rctg Bn should enroll at least one person into DITMS. The designated individual will be the focal point for that organization who will designate all excess ITE in DITMS for that organization to transfer to other DOD organizations or schools who are registered with the Computers for Learning web site. Enrollment in DITMS requires the submission of DISA Form 41 (System Authorization Access Request (SAAR)). The form is available on-line and is used to verify the designated individual's clearance and justification for access to DITMS. The form can be faxed to the DITMS Office, but the original must be mailed at the earliest possible date. Upon receipt of the user ID and password, the individual can begin entering the equipment into the system. All ITE must be entered into the system regardless of its final disposition. More information can be found at the DITMS web site, www.disa.mil/cio.darmp.ditmsap.

e. Schools. Automation equipment can be turned in and redistributed to schools under the Educational Institution Partnership Program (EIPP). The EIPP is authorized by Executive Orders 12999, 12900, 12876, 13021, and 13096 and is part of the Defense Automation Resources Management Program. The Defense Special Programs Division of the Chief Information Officer governs EIPP. Schools must first register with the Computers for Learning web site at www.computers.fed.gov. This web site is designed specifically for schools and eligible non-profit organizations to register to receive excess Government ITE, not only from DOD, but from other Federal agencies as well. The requesting school must then submit a written memorandum requesting the hardware and/or software. The memorandum must include the number of computers requested, that the computers will be used for mathematics or science, and that the com-

puters will be in school for at least 1 year. The IM point of contact will enter the items in DITMS to ensure that no other DOD organization has a need for the equipment. After a 30-day holding period if no other DOD organization has a need for the equipment, DITMS will authorize the IM point of contact or PBO to release the equipment to the requesting education (nonprofit) organization. The receiving organization is responsible for making transportation arrangements.

Chapter 5 Systems Assurance

5-1. Purpose

To control and manage IM configuration items throughout the life cycle of each separately designated system through use of the three disciplines of CM, quality assurance, and test and evaluation.

5-2. Scope

All IM systems whether contracted or developed in-house will be subject to the USAREC-Army National Guard CM. This requires development of a CM plan that incorporates a CCB, a charter, definition of each configuration item whether hardware, software, or documentation (including drawings), a change control procedure, a numbering system for tracking configuration items (that provides for linking hardware, software, and documentation), and a reporting system that indicates the status of each configuration item. A quality assurance plan will be developed that defines the applicable standards to be used prior to acceptance of each configuration item. A test and evaluation plan will be developed that states what test criteria will be applied to each configuration item prior to acceptance or rejection. Finally, an overall flowchart will be developed describing the process of an item from receipt to acceptance. This chart will identify organizations, forms, reports, and procedures necessary to administer each configuration item over the life cycle of the system.

5-3. Responsibility

Each technical integrated product team (IPT) leader or the Chief of Application Program Division, Information Management Directorate, is responsible for defining the necessary resources, to include early and continuous information assurance coordination to accomplish this policy. It is the responsibility of the Chief of Resource Management and Plans Division, Information Management Directorate, to provide any additional personnel or funding to implement this policy. The Director of Information Management is responsible for granting any waiver from this policy due to lack of resources or other exigencies.

5-4. Authority

The technical IPT leaders will have sole authority as to the level of detail that the configuration items will be defined. Any changes requiring additional funding will not be approved without concurrence of Chief of Resource Management and Plans Division, Information Management Directorate. All approved changes require the signature of the Director of Information Management or his or her designated representative.

Chapter 6 Communications

6-1. Telecommunications

Procedures for requesting and managing communications equipment and/or services is provided in USAREC Reg 25-10.

6-2. E-mail

USAREC employees will employ Government-owned e-mail systems for authorized unclassified Government business. USAREC employees will not use unapproved accounts (such as Hotmail or Yahoo mail) for official business unless specifically authorized to do so by the Director of Information Management. USAREC employees shall not transmit classified information over any communications system unless it is transmitted using approved security procedures and practices. USAREC employees should exercise extreme care when transmitting any sensitive information or other valued data. Guidance for requesting and usage of e-mail services is provided in USAREC Reg 25-11.

6-3. Electronic bulletin boards

Electronic bulletin boards can be used to disseminate information to users. Information placed on the Official Bulletin Board is limited to FOUO messages. Information placed on the Unofficial Bulletin Board is limited to general public information. Additional guidance governing the use of bulletin boards and a more detailed explanation of authorized messages is provided in USAREC Reg 25-11.

a. The Unofficial Bulletin Board exists to provide military and civilian employees of HQ USAREC with a convenient medium for the exchange of unofficial information about the sale or exchange of personal property, the solicitation of assistance with lawful personal activities, notice of community events, and public service announcements.

b. Both the Unofficial Bulletin Board and the time and productivity of the employees in HQ USAREC are valuable Government resources. The premise underlying the Unofficial Bulletin Board is that employees may announce and learn of unofficial information more efficiently and with less impact on their Government work than through other similar means of information exchange. Thus, items posted to the board should be brief (generally one e-mail entry screen or less), not only because postings consistent

with the Unofficial Bulletin Board's purpose will by their nature be brief, but also because this minimizes the diversion from Government duties of both the author and the readers.

c. The following are examples of authorized uses of the Unofficial Bulletin Board. While these examples are not intended to be exclusive, any proposed posting not clearly within the following categories should be coordinated in advance with the e-mail administrator:

(1) Sale, purchase, or exchange of personal, nonbusiness property in noncommercial quantities.

(2) Public service announcements such as personal items lost or found, car lights left on or car alarms operating, under circumstances suggesting USAREC employee ownership, requests for donation of annual leave in support of USAREC employees, and information about donating time, money, or property to disaster assistance efforts or to charities endorsed under DOD 5500.7-R (e.g., Combined Federal Campaign, Army Emergency Relief).

(3) Announcements of command functions, farewell luncheons, and other community and/or organization events that are either open to the public or sponsored by nonprofit entities.

d. The following are examples of unauthorized uses of the Unofficial Bulletin Board which are unauthorized because they are outside the scope of intended usage of the board or because they violate law or regulation:

(1) Endorsement of businesses of furtherance of commercial enterprises. This includes notices of commercial sales or money-saving opportunities which, while apparently benign, can also create the perception of a misuse of position by the author for private gain by virtue of a hidden relationship with the vendor.

(2) Statements or commentaries of personal belief or opinion or observations unrelated to an authorized use as noted above, or the recitation of such beliefs, opinions, or observations of others, on any subject. Numerous commercial online services are available for this kind of activity, which is purely personal and beyond the intended scope of the Unofficial Bulletin Board.

(3) Statements, commentaries, or declarations of support on any subject which are intended to invite, or by their nature may reasonably be understood to invite, responses by readers.

(4) The telling of jokes, anecdotes, testimonies, stories, or other similar matters.

6-4. Internet and Intranet

Internet access is defined as the ability to connect to and acquire information contained at Internet sites. Rctg Bdes and Rctg Bns are only authorized to access the Internet over the Recruiter Services Network backbone and approved Internet service provider.

a. Internet web presence. Web presence is defined as posting information or content that is accessible via the Worldwide Web using a browser. This presence is commonly known as hosting a web site or page. Rctg Bdes, Rctg Bns, recruiting companies, and RS are not au-

thorized to maintain a web presence with a commercial provider or vendor. Official command information that is intended for public access will be hosted by HQ USAREC, Rctg Bdes, and Rctg Bns on <http://www.usarec.army.mil>. Information down to RS levels posted on this site by HQ USAREC, Rctg Bdes, and/or Rctg Bns must comply with DOD and DA policies covering the publicly accessible web sites. DOD policies can be found at <http://www.defenselink.mil/admin/about.html#WebPolicies>. DA policies can be found at http://www.army.mil/DA_web_guidance.htm. HQ USAREC and Rctg Bde and Rctg Bn commanders are responsible for information posted on the <http://www.usarec.army.mil> site. All information should be reviewed by the unit's advertising and public affairs officer prior to posting to ensure compliance. USAREC units and persons assigned to or affiliated with USAREC, with the exception of HQ USAREC, Advertising and Public Affairs Directorate, are not authorized to maintain a web presence for the purposes of disseminating Army marketing communications information. Personal or individual homepages that advertise or allude to an affiliation with USAREC are prohibited.

b. Intranet. All command employees with Recruiter Services Network access shall use the command Intranet to access, search, and share command and control information. The USAREC Intranet operates on a private Government network that is fully secured and protected by a firewall. HQ USAREC, Rctg Bde, and Rctg Bn sites will be equipped with software and hardware that will enable them to host information to their respective unit. Each unit is responsible for maintaining the hyper text markup language materials (content) on their server or assigned directory. Each unit shall identify a primary point of contact or webmaster. Directorate webmasters shall represent their unit during Intranet Operations Board meetings. Rctg Bde and Rctg Bn webmasters concerns and suggestions should be addressed to the USAREC web administrator who will present them to the Internet and Intranet Technical Working Group. The Internet and Intranet Technical Working Group is a working group which functions under the direction of the CCB. Unit webmasters may identify additional personnel within their unit to serve as pagemasters. Pagemasters are usually responsible for maintaining specific subareas.

c. The Internet provides a tremendous resource of information interchange and other communication. Subject to the restrictions stated in paragraph 4-8, Government IT systems may be used to access USAREC Internet resources for professional development purposes, subject to ensuring that primary duties and missions are accomplished. Government IT systems may also be used to access and use these internet resources for limited periods of time for other personal reasons such as finding and reading professional literature or checking stock quotes

and other nonproscribed web sites. Such use, however, should be limited to before or after work hours or during lunch or other authorized breaks during the workday.

Chapter 7

Audiovisual and Video Teleconferencing Support

7-1. Responsibilities

This chapter describes capabilities and procedures for audiovisual and video teleconferencing (VTC) support within USAREC.

a. HQ USAREC. For HQ USAREC, Information Management Directorate's audiovisual coordinator and VTC coordinator are responsible for assisting, installing, maintaining, operating, and troubleshooting audiovisual and VTC assets respectively.

b. Rctg Bdes and Rctg Bns. At the Rctg Bde and Rctg Bn level, the respective IMO or IMS is responsible for assisting, installing, maintaining, operating, and troubleshooting USAREC audiovisual and VTC assets.

7-2. Capabilities

a. Audiovisual facilities (building 1307). HQ USAREC has one command conference room (CCR), one deputy commanding general conference room (DCGCR), three small conference or classrooms, and a multimedia room. Each of these areas has electronic equipment associated with it that is owned and operated by Information Management Directorate's audiovisual coordinator. Information for scheduling any of these areas can be obtained by contacting the audiovisual coordinator telephonically or by e-mail. The CCR seats approximately 100 persons; the other rooms seat approximately 10 to 20 persons each.

b. Audiovisual equipment (building 1307 and loaners).

(1) Fixed-position equipment. The CCR and DCGCR are equipped with audiovisual equipment which includes ceiling-mounted projectors, videocassette recorders, visual presenters, videotaping equipment, LAN-connected computers, and compact disk players. Both rooms also have public address systems and ceiling-mounted speakers. A full description of technical equipment can be obtained by contacting the audiovisual coordinator.

(2) Portable equipment. The audiovisual coordinator possesses a limited inventory of audiovisual devices for use outside the headquarters building. Equipment currently in the inventory includes conventional overhead projectors, portable liquid crystal display projectors, and a videocassette recorder. A full description of equipment can be obtained by contacting the audiovisual coordinator. Operator training is provided for all portable equipment.

c. VTC facilities (building 1307). At HQ USAREC the CCR, DCGCR, conference rooms 1 and 2, and the advertising and public affairs multimedia room are equipped to support VTC

connections (i.e., Integrated Services Digital Network Basic Rate Interface circuit terminated on a registered jack (RJ) 45). The CCR can seat approximately 100 persons and the remaining conference rooms can seat between 10 and 20 people.

d. VTC equipment.

(1) Fixed-position equipment (building 1307). The headquarters CCR is equipped with a fixed VTC system capable of projecting its output on the large screens for large audience viewing.

(2) Roll-about equipment.

(a) At HQ USAREC the DCGCR, conference rooms 1 and 2, and the advertising and public affairs multimedia room are each set up to accept roll-about VTC units. There are six roll-about systems at the headquarters.

(b) Each Rctg Bde has two roll-about systems and a desktop unit. Each Rctg Bn has one roll-about system and a desktop unit.

7-3. Support scheduling

a. Facility scheduling.

(1) CCR. The CCR is scheduled through the HQ USAREC Protocol Office.

(2) DCGCR. The DCGCR is located on the second floor and is scheduled by the Deputy Commanding General-West administrative officer.

(3) Conference rooms 1 and 2. These rooms are located on the third floor and are scheduled through the Headquarters Company's office.

(4) Advertising and Public Affairs Directorate's multimedia room. This room is located on the first floor, and can be scheduled through the Advertising and Public Affairs Director's secretary.

b. Audiovisual assistance and/or equipment. Visual Information equipment, operator training, conference room support, and other audiovisual assistance is requested by contacting the audiovisual coordinator by e-mail or telephone. Requests should be made in as timely and complete manner as possible. Upon receipt, an audiovisual coordinator representative will contact the requester to verify support, discuss technical requirements, etc.

c. VTC assistance and/or scheduling. Contact the Information Management Directorate's VTC coordinator. Coordinating and setting up the video bridge for a multipoint or point-to-point VTC requiring a bridge (i.e., private to commercial) requires 5 working days advance notice. Point-to-point VTC that do not require a bridge (commercial to commercial) are not as complicated to set up and require only 3 working days advance notice. To facilitate set up of a VTC, the VTC coordinator will require completion of USAREC Form 1207 (USAREC Video Teleconference (VTC) Request) (see fig 7-1).

Chapter 8 Administrative Services

8-1. Administrative Services Branch

The following disciplines are under the manage-

ment of the Chief of Administrative Services Branch, Information Management Directorate:

a. The Freedom of Information Act Program (AR 25-55).

b. The Army Privacy Act Program (AR 340-21 and DA Pam 25-51).

c. The Official Mail and Distribution Management Program (AR 25-51 and the Domestic Mail Manual (DMM)).

d. The Records Management Program.

e. Publications, forms, and printing management.

f. Office automation.

8-2. Office automation

a. Office automation under the Administrative Services Branch, Information Management Directorate, consists of the following disciplines:

(1) ITE (PC, printers, digital cameras, scanners).

(2) Records management support equipment (copiers, micrographics, visual information approvals).

b. The following regulatory guidance establishes controls and operates the above disciplines:

(1) AR 25-1.

(2) AR 25-30.

8-3. Records management procedures and inspections

Records management under the Administrative Services Branch, Information Management Directorate, consists of the following disciplines for survey purposes or control as indicated:

a. Correspondence and distribution management (AR 25-50).

b. Management information control (survey only).

c. Forms management (survey only).

d. Publications and printing management (survey only).

e. Official mail management (survey only).

f. Office equipment (files) management (AR 25-1).

g. Files maintenance, utilization, and disposition management (AR 25-400-2).

h. Freedom of Information Act Program (survey only).

i. Privacy Act Program (survey only).

8-4. Publications, forms, and printing management

Publications, forms, and printing management under the Administrative Services Branch, Information Management Directorate, consists of the following disciplines:

a. Publications management (AR 25-30 and USAREC Pam 25-30).

b. Forms management to include electronic forms (AR 25-30 and USAREC Pam 25-30).

c. Printing management (AR 25-30).

d. Management information control (AR 335-15).

e. Recruiter business card management (USAREC Reg 25-30).

Chapter 9 Systems Documentation

9-1. Purpose

Provide uniform guidelines in accordance with IEEE/EIA 12207 for the development and revision of documentation for AIS and specify the content of each of the core documents that must be produced during the life cycle of AIS. Additional product description documents or project-unique documents (i.e., system interface agreements, joint application design, high-level requirements matrix, etc.) may be required based on the determination of the assigned project manager (PM).

9-2. Scope

These standards apply to both internal and contractual development efforts by the Information Management Directorate, and to the managers and technicians at all levels concerned with the development, modification, operation, testing, implementation, and maintenance of an AIS or stand-alone application software. These standards cover required technical documents for an AIS, application software, and revisions.

9-3. Responsibility

The Chief of Application Program Division, Information Management Directorate, or assigned PM is responsible for assuring that AIS documentation standards are applied. Brief descriptions of the required documentation follow:

a. Software requirements specifications (SRS).

(1) Preparation. SRS specify the requirements for a computer software configuration item (CSCI) and the methods to be used to ensure that each requirement has been met. Requirements pertaining to the CSCI's external interfaces may be presented in the SRS or in one or more interface requirement specifications (IRS) referenced from the SRS.

(2) Uses. The SRS, possibly supplemented by IRS, is used as the basis for design and qualification testing of a CSCI.

b. IRS.

(1) Preparation. The IRS specifies the requirements imposed on one or more systems, subsystems, hardware configuration items, CSCI, manual operations, or other system components to achieve one or more interfaces among these entities. An IRS can cover any number of interfaces.

(2) Uses. The IRS can be used to supplement the system or subsystem specification and the SRS as the basis for design and qualification testing of systems and CSCI.

c. Software design description (SDD).

(1) Preparation. The SDD describes the design of a CSCI. It describes the CSCI-wide design decisions, the CSCI architectural design, and the detailed design needed to implement the software. The SDD may be supplemented by the interface design descriptions and database design descriptions.

(2) Uses. The SDD with its associated interface design descriptions and data base design descriptions is used as the basis for implementing the software. It provides the acquirer visibility into the design and provides information needed for software support.

d. Software test plan (STP).

(1) Preparation. The STP describes plans for qualification testing of CSCI and software systems. It describes the software test environment to be used for the testing, identifies the tests to be performed, and provides schedules for test activities.

(2) Uses. There is usually a single STP for a project. The STP enables the acquirer to assess the adequacy of planning for CSCI and if applicable, software system qualification testing.

e. Software test description (STD).

(1) Preparation. The STD describes the test preparations, test cases, and test procedures to be used to perform qualification testing of a CSCI or a software system or subsystem.

(2) Uses. The STD enables the acquirer to assess the adequacy of the qualification testing to be performed.

f. Software test report.

(1) Preparation. The software test report is a record of the qualification testing performed on a CSCI, a software system or subsystem, or other software-related item.

(2) Uses. The STD enables the acquirer to assess the testing and its results.

g. Software center operator manual (SCOM).

(1) Preparation. SCOM provides personnel in a computer center or other centralized or networked software installation information on how to install and operate a software system.

(2) Uses. The SCOM is developed for software systems that will be installed in a computer center or other centralized or networked software installation, with users accessing the system via terminals or PC or submitting and receiving inputs and outputs in batch or interactive mode.

h. Software user manual (SUM).

(1) Preparation. The SUM tells a hands-on software user how to install and use a CSCI, a group of related CSCI, or a software system or subsystem. It may also cover a particular aspect of software operation, such as instructions for a particular position or task.

(2) Uses. The SUM is developed for software that is run by the user and has a user interface requiring on-line user input or interpretation of displayed output. If the software is embedded in a hardware or software system, user manuals or operating procedures for that system may make separate SUM unnecessary.

9-4. Authority

The Chief of Application Program Division or assigned PM has the authority to expand or increase the level of documentation described above, if needed, for complex AIS and/or application software.

Chapter 10 Preventive Maintenance and Housekeeping

10-1. Sites

There are over 2,000 sites in USAREC that have

ITE installed. The sites range from large mainframe computer installations to desktop micro-computers. No matter the size, they all require periodic preventive and remedial maintenance.

10-2. Cost

One major factor in the cost of maintenance is the required service performed as a result of poor housekeeping around the equipment. Equipment has been needlessly damaged by spilled drinks, food particles, paper clips, staples, etc.

10-3. Policy

It is the policy of this command that all users of ITE or peripheral equipment will not permit food or drink at ITE workstations, nor will food or drink be placed upon peripheral equipment. Paper clips or staples will not be placed on or around equipment. Magnets can also harm electronic equipment and should never be placed in close proximity to electronic equipment.

10-4. Inspections

Commanders will include preventive maintenance and housekeeping as an inspection item during their command inspections.

Chapter 11 Procedures for Preparation and Processing of System Change Requests

11-1. Submission form

There is a standing operating procedure to process a request to change an existing USAREC software baseline, to create a new baseline, or for a documentation change. These requests are submitted using HQ USAREC Form 1913. The current USAREC baseline consists of the Army Recruiting Command Central Computer System (ARC3S), microcomputer applications, Army Recruiting and Accession Data System, and ARISS.

11-2. Submission process

HQ USAREC Form 1913 will normally originate from HQ USAREC directorates who are functional proponents or the Army National Guard Liaison Office. Normally, HQ USAREC Form 1913 will be prepared by the SME often working with a functional integrated product team (FIPT) leader and a computer specialist or software engineer. The FIPT leader should, if possible review and approve the system change request (SCR) prior to submission to HQ USAREC (RCIM-CM).

NOTE: The Information Management Directorate's homepage web site on the USAREC Intranet also contains a copy of the SCR submission standing operating procedure. All software requests will be forwarded to HQ USAREC (RCIM-CM). The SCR is forwarded by e-mail (e-mail address is (CM-SCR)) or entered into the CM system via our CM software application, Tracker. Electronic supporting documentation for the SCR should be attached to SCR e-mail message submission. Hard copy documentation should be forwarded to HQ USAREC (RCIM-CM) through distribution. HQ USAREC (RCIM-CM) is responsible for providing documentation to the technical IPT and FIPT before the CCRB. New

SCR and impact analyses received after 1200 on the Friday immediately before the CCRB will not be presented at that CCRB but will be presented at a subsequent CCRB.

11-3. CM Office processing

The SCR will be reviewed by the Information Management Directorate, CM Office, to assure proper completion. If there is a problem with the SCR, the CM Office will contact the submitter and the problem will be resolved prior to posting on Tracker. CM Office, will post the SCR on Tracker, assign a tracking number, and schedule the SCR for a CCRB. The CM Office will provide a copy of the agenda and the location of the CCRB to the submitter. The CM Office will provide a copy of the agenda to the technical IPT lead and FIPT lead. If the technical IPT lead is not identified on the SCR, the CM Office should contact the submitter or the appropriate manager (e.g., Chief of Application Program Division) to identify the technical IPT lead. The CM Office will also provide agendas to other appropriate individuals. On the day of the scheduled CCRB, the FIPT and the technical IPT leader, if identified, will attend. The CCRB chairperson will ask the FIPT to explain the purpose of the request, anticipated impact, expected completion date, etc. The assigned technical IPT leader will assist in describing the request. The CCRB will take action on the SCR.

11-4. Impact analysis

If the SCR is accepted by the CCRB, it will be assigned to a technical IPT lead for the development of an impact analysis. The CCRB will establish the date when the impact analysis is due (usually 2 weeks after the CCRB). The CM Office will provide an agenda to the FIPT and technical IPT lead of the CCRB time and date designated to discuss the impact analysis. The FIPT leader and technical IPT leader will participate in the review of the impact analysis at the designated CCRB. Based on this review the SCR will be accepted, tabled, deferred, or rejected. If rejected the submitter may request review by the CCB. If this is so, the CM Office will schedule the action with the CCB executive secretary, who will place the item on the CCB agenda and notify all concerned parties prior to the scheduled CCB.

11-5. Approved request

If the request is accepted, it is assigned to a technical IPT leader and forwarded to the appropriate PM for cost and schedule consideration. (For all non-ARISS application development the PM is the Chief of Application Program Division.) If the PM approves the request, the technical IPT leader will assign team resources and create the project schedule in conjunction with the SME and the FIPT leader.

11-6. Documentation

Documentation (per chap 9) will be submitted electronically to HQ USAREC (RCIM-CM) for review and approval. Documentation products will be annotated for correction if necessary and returned to the submitter. Storage and management of in-process materials is the responsibility

of the technical IPT leader.

11-7. Development

The Application Program Division is using the project management methodology to conduct software engineering projects. Requirements of this methodology are provided in periodic development training sessions for personnel. A complete description of the methodology is available on Information Management Directorate's Homepage for anyone who wants an indepth view. The tools involved in software engineering are rapidly evolving. Choice of software development tools is project specific and requires the prior approval of the Chief of Application Program Division. Another aspect of software development is the attainment of superior software development processes. A software organization's processes can be measured against a profile termed the capability maturity model. This model was developed by the Software Engineering Institute and was sponsored by DOD. Through the use of the model, capability levels are determined based on a five-level scale, with five being the best. A more complete explanation is available on the Information Management Directorate's Intranet Homepage.

11-8. Close project

The project will not be considered complete and the SCR will not be closed until all products and documentation are approved through the CM approval process.

11-9. Implementation

Release dates will be coordinated by Application Program Division with developers, operations, and the proponent or user authority. Application Program Division will ensure that all documentation, coordination, and notification is ready and in place before the release for production is scheduled. Application Program Division will ensure that all documentation, coordination, and notification is ready and in place before the release for production is scheduled.

Chapter 12 Systems Support

12-1. General

Information Management Directorate currently staffs the SOC which is continually manned except for Thanksgiving, Christmas, and New Years. An individual will answer the telephone and accept verbal or electronic requests for service, repair, warranty, and/or troubleshooting. They will create a trouble ticket which will be used to track the call and its successful conclusion. Historical data will be available on the LAN for requesters to obtain status. This capability will improve the quality and accuracy of requests as they are tracked through the system. Call the SOC at DSN 536-1700 or 1-(800)-223-3735, extension 61700. Emergency assistance during holiday periods can be obtained by contacting the staff duty noncommissioned officer and having an Information Management Directorate rep-

resentative paged.

12-2. SOC

The Information Management Directorate mans the SOC which is responsible for managing problems related to the LAN, wide area network, e-mail, telephone equipment, PC hardware including printers and software, and ARC3S. They monitor the servers and respond automatically to outages and initiate action necessary to restore service and/ or data. The SOC has personnel who receive problem calls and enter them into a remedy tracking database. Those calls that they receive and cannot immediately assist are redirected electronically, and sometimes by voice, along with the entered problem reports with all data initially collected. The SOC will develop a methodology to determine the location to which referred problem reports should be directed. The data entry file will be used to track the call and its successful conclusion. Historical data will eventually support expert system prompts on possible remedies which can be applied to fix problems. This capability will improve as the quality of accurate and complete data increases. Locations receiving immediate redirect when problems cannot be solved will be the Communications-Electronics Division, Application Program Division (ARC3S), Systems Integration Office, and the Help Desk.

12-3. Help Desk

The Information Management Directorate, Support Operations Branch personnel function as an HQ USAREC Help Desk. They take calls and electronic data forwarded by the SOC and take action in priority to remedy the problems redirected. Generally, they will physically go to the sites that have a problem which cannot be resolved by telephone and which deal with automated systems from the wall plug outward. They will coordinate with the Communications-Electronics Division for items inward from the wall plug. Other areas of responsibility include evaluation, configuration, installation, and compatibility testing of PC hardware and software to assist in fielding of PC equipment at the headquarters and field. The Help Desk is also responsible for managing the Information Management Directorate's Training Lab. Scheduling is through the Help Desk calendar; send an e-mail to IM Tech Support@usarec.army.mil or call 1-(800)-223-3735, ext. 60014 and check for availability.

12-4. CM

A discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements. The Information Management Directorate, CM Office, currently provides varying levels of CM support for several USAREC systems. The CM Office also provides repository support for several projects through the Knowledge Center Repository. The CM Office's support includes reviewing SCR, facilitating CCRB meetings, administering configuration item approval process,

administering the CM library (also known as the Knowledge Center Repository), and tracking all SCR.

12-5. Quality assurance

Quality assurance is a planned and systematic pattern of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements. It is a set of activities designed to evaluate the process by which products are developed or manufactured. The Software Quality Assurance Team shares management and administrative duties such as creating an ARISS software quality assurance plan, creating ARISS software quality assurance checklists, conducting reviews and audits, developing metrics, and providing management briefings.

12-6. Risk management

The developer will perform risk management throughout the software development process. The developer will identify, analyze, and prioritize the areas of the software development project that involve potential technical, cost, or schedule risks; develop strategies for managing those risks; record the risks and strategies in the software development plan; and implement the strategies in accordance with the risk management plan. The risk management plan serves as the guidance in applying risk management to all future command development projects requiring the application of risk management.

12-7. Test and evaluation

Testing is an activity in which a system or component is executed under specified conditions, the results are observed and recorded, and an evaluation is made on some aspect of the system component. All IM software products will be tested, evaluated, and approved by the Information Management Directorate prior to release to users.

12-8. Release management

Release management is the discipline that assures that the software being sent to the customer has been tested, approved, fully described, documented, scheduled, coordinated, and distributed. The SVD document is used in this process.

12-9. Data standards

See AR 25-1 and DOD 8320.1-M-1 for data standards policies and procedures.

REQUIREMENTS STATEMENT (For use of this form see USAREC Reg 25-2)		1. REQUEST # 01-RMP-0001	2. DIRECTORATE # RMP-001	3. REQUEST DATE 30 Nov 2000
4. DESCRIPTION: Computer equipment for new hire.				
5. REQUIREMENT: Computer with monitor, keyboard, printer, and office automation software.				
6. JUSTIFICATION: The Acquisition and Contracts Branch has recently hired a new employee and requires automation equipment and software to support the new position.				
7. HQ PROPONENT & RECOMMENDATION:		RMP	==>	Y
8. IM POC & RECOMMENDATION:		Bates	==>	Y
9. ITEMS REQUIRED:	QTY	COST	SUBTOTAL	
01: CPU	1 X	\$1,500.00	\$1,500.00	
02: Laserjet Printer	1 X	\$400.00	\$400.00	
03: MS Office	1 X	\$400.00	\$400.00	
04:				
05:				
06:				
07:				
08:				
09:				
10:				
		TOTAL COST= = > \$2,300.00		
10. REQUESTING AUTHORITY: (SIGNATURE/DATE) (TYPED NAME, RANK/GRADE, TITLE & TELEPHONE)		11. REQUESTING AGENCY IM O/POC: (SIGNATURE/DATE) (TYPED NAME, RANK/GRADE, TITLE & TELEPHONE)		
BRUCE W. MORRIS, GS-14, CH, RMP (502) 626-0646		ROGER K. BATES, GS-13, CH, RMP-A (502) 626-0653		
12. PURCHASE TYPE: Out-of-Cycle Purchase		15. ACTION OFFICE: RMP		
13. ACTION PENDING: New Request		16. ACTION OFFICER: Bates		
14. APPROVAL AUTH: Director, IM		17. PRIORITY #:		

Figure 2-1. Sample of a completed USAREC Form 1089

SYSTEM CHANGE REQUEST (For use of this form see USAREC Reg 25-2)	
* Required fields. Double click on a field for Help Information.	
* CHANGE TITLE: MEPCOM Nightly File Transfer Migration	
* LIST AFFECTED SYSTEMS, SUBSYSTEMS, OR ITEMS:	
* CHANGE DESCRIPTION: Migrate the nightly file transfer from Prime to GC NT computers.	
NEED FOR CHANGE: Prime computers are at the end of their life cycle and as many functions as possible should be migrated away from the Prime computers to reduce the risk due to age and condition of Prime computers.	
PRIORITY: <input type="checkbox"/> To Be Determined <input type="checkbox"/> Urgent <input checked="" type="checkbox"/> Routine <input type="checkbox"/> Emergency	
* SUBMITTER NAME: J. Richards	TELEPHONE: 6-1303
* FUNCTIONAL LEAD: MSG Klinger	TELEPHONE:
TECHNICAL LEAD: Nikki LeClerc	TELEPHONE: 6-0029
FUNCTIONAL SME:	TELEPHONE:
ORGANIZATION: IM	
* SUBMIT DATE: 6 Jan 2000	
STATUS: AWT CCRB	
WBS CODE:	
CLASS: <input checked="" type="checkbox"/> Class I (Example: Change has an Impact to Schedule) <input type="checkbox"/> Class II (Example: Documentation Change)	
NOTE: Send this completed form to RCIM -CM-SCR via e-mail. Please contact ARISS CM office if you do not receive a reply to your e-mail with a control number for your change request.	

Figure 2-2. Sample of a completed HQ USAREC Form 1913

USAREC VIDEO TELECONFERENCE (VTC) REQUEST

(For use of this form see USAREC Reg 25-2)

1. CONFERENCE TITLE: Production VTC		2. DATE OF REQUEST: 1 Dec 2000	
3. SENIOR ATTENDEE: MG Cavin			
4. VTC DATE: 18 Dec 2000	5. VTC TIME: 1030 Eastern	6. VTC LENGTH: HOURS 1	MINUTES 30
For assistance or additional information contact the VTC coordinator located at Headquarters, U.S. Army Recruiting Command, Information Management Directorate, (800) 223-3735, ext. 61474.			
7. PRIMARY POC: Roger Emery		8. OFFICE: RCIM	
9. E-MAIL ADDRESS: Roger.Emery@usarec.army.mil			
10. TELEPHONE: COMMERCIAL: (502) 626-1474		DSN: 536-1474	FAX: (502) 626-0913
11. ALTERNATE POC: Jim Welker		12. OFFICE: RCIM	
13. E-MAIL ADDRESS: WelkerJ@usarec.army.mil			
14. TELEPHONE: COMMERCIAL: (502) 626-0625		DSN: 536-0625	FAX: (502) 626-0913
15. VTC LOCATION: <input type="checkbox"/> CCR <input checked="" type="checkbox"/> DCGCR <input type="checkbox"/> CONF ROOM 1 <input type="checkbox"/> CONF ROOM 2 <input type="checkbox"/> OTHER (specify): _____			
16. VTC TYPE: POINT-T0-POINT <u> X </u> MULTIPOINT _____			
17	18	19	20
CONFERENCE LOCATION	ROOM ID AND TELEPHONE NUMBER	VTC TELEPHONE NUMBER	ATTENDEE NAME AND TELEPHONE NUMBER
Fort Knox, KY	DCG Conference Room (502) 626-1656	(502) 799-1602	MG Cavin (502) 626-0605
Fort Sam Houston, TX	Conference Room (210) 444-0101	(210) 444-1789 (210) 444-1794	COL Whitley (210) 444-0601

USAREC Form 1207, 1 Dec 2000

V1.00

Figure 7-1. Sample of a completed USAREC Form 1207

Appendix A
References

Section I
Related Publications

AR 25-1

Army Information Management.

AR 25-30

The Army Publishing and Printing Program.

AR 25-50

Preparing and Managing Correspondence.

AR 25-51

Official Mail and Distribution Management.

AR 25-55

The Department of the Army Freedom of Information Act Program.

AR 25-400-2

The Modern Army Recordkeeping System (MARKS).

AR 335-15

Management Information Control System.

AR 340-21

The Army Privacy Program.

AR 380-19

Information Systems Security.

AR 710-2

Inventory Management Supply Policy Below the Wholesale Level.

AR 735-5

Policies and Procedures for Property Accountability.

DA Pam 25-51

The Army Privacy Program - System of Records Notices and Exemption Rules.

DOD 5500.7-R

Joint Ethics Regulation (JER).

DOD 8320.1-M-1

Data Element Standardization Procedures.

DMM

Domestic Mail Manual.

FAR

Federal Acquisition Regulation.

IEEE/EIA 12207

Information Technology Software Life Cycle Processes.

UCMJ

Uniform Code of Military Justice.

USAREC Reg 25-10

Telecommunications Management.

USAREC Reg 25-11

CC:Mail Management Program.

USAREC Reg 25-30

Recruiter Business Cards.

USAREC Reg 735-3

Supply Procedures.

USAREC Pam 25-30

Index, Distribution, and Resupply of USAREC Publications and Blank Forms.

Section II
Required Forms

USAREC Form 1089

Requirements Statement.

USAREC Form 1207

USAREC Video Teleconference (VTC) Request.

HQ USAREC Form 1913

System Change Request.

USAREC Label 23

Property of the U.S. Army.

Section III
Related Forms

DD Form 1348-1A

Issue Release/Receipt Document.

DD Form 1556

Request, Authorization, Agreement, Certification of Training, and Reimbursement.

DD Form 1610

Request and Authorization for TDY Travel of DOD Personnel.

DISA Form 41

System Authorization Access Request (SAAR).

SF 120

Report of Excess Personal Property.

Glossary

Section I Abbreviations

AIS

automated information systems

ARC3S

Army Recruiting Command Central Computer System

ARISS

Army Recruiting Information Support System

BOI

basis of issue

CAPR

capability request

CCB

Configuration Control Board

CCR

command conference room

CCRB

change control review board

CM

configuration management

CofS

Chief of Staff

CSCI

computer software configuration item

DA

Department of the Army

DCGCR

deputy commanding general conference room

DISC4

Director of Information Systems for Command Control, Communications, and Computers

DITMS

Defense Information Technology Management System

DOD

Department of Defense

DRMO

Defense Reutilization Management Office

EIPP

Educational Institution Partnership Program

FIPT

functional integrated product team

FOUO

For Official Use Only

FY

fiscal year

GOV

Government-owned vehicle

HQ USAREC

Headquarters, United States Army Recruiting Command

IAM

information assurance manager

IAO

information assurance officer

ID

identification

IM

information management

IMAWG

Information Management Advisory Working Group

IMO

information management officer

IMS

information management specialist

IMSC

Information Management Support Council

IPT

integrated product team

IRM

information resources management

IRS

interface requirement specifications

ISA-USAREC

United States Total Army Personnel Command Information Support Activity - United States Army Recruiting Command

IT

information technology

ITE

information technology equipment

LAN

local area network

PBO

property book officer

PC

personal computer

PHRH

primary hand receipt holder

PM

project manager

POV

privately-owned vehicle

Rctg Bde

recruiting brigade

Rctg Bn

recruiting battalion

RS

recruiting station

Rs Bde

United States Army Recruiting Support Brigade

RWS

recruiter workstation

SA

system administrator

SCOM

software center operator manual

SCR

system change request

SDD

software design description

SME

subject matter expert

SOC

Service Oversight Center

SRS

software requirements specification

STD

software test description

STP

software test plan

SUM

software user manual

SVD

software version description

USAREC

United States Army Recruiting Command

VTC

video teleconferencing

Section II

Terms

account number

Number assigned to users for control and monitoring of usage of IM computers.

activity

A DA recruiting unit or organization performing a specific function.

Army Recruiting and Accession Data System

A USAREC network of communication and automation assets designed to create and process the single source applicant record as well as other management support information (i.e., advertis-

ing, personnel, finance, etc.).

contiguous group of information technology equipment

Any ITE which is located in close proximity. For example: A duty section or branch where one individual would be able to reasonably maintain awareness of ITE use and security.

contracting officer

A military or DA civilian employee who has been delegated authority for the execution, distribution, and administration of all telecommunications service contracts within a designated area, consisting of one or more Army installations or activities. Authority for such contracting will be in accordance with procedures outlined in the Federal Acquisition Regulation (FAR).

contracting officer's representative

A military or DA civilian employee who has been appointed by a contracting officer, in writing, to act as their authorized representative in administering a contract. The written designation will clearly define the scope and limitations of the authority delegated to the contracting officer's representative.

economic analysis

An analysis of stated communications-electronics requirements to ensure the most cost-effective alternative which satisfies the requirement and is consistent with Army objectives and practices is selected.

information assurance officer

Individual designated in writing to ensure effective implementation of applicable automation security regulations at the IM data processing activity, and is the central point of contact to manage the control and dissemination of file identification numbers and passwords for users of terminals and devices interconnected with the IM host computer systems.

Information Management Advisory Working Group

A group comprised of director and commander designated representatives from each HQ USAREC directorate, special staff section, and Rctg Bde. The IMAWG will conduct periodic reviews of Information Management Directorate's IT plans which itemize all outstanding requests for Information Management Directorate support as well as initiatives. The IMAWG charter contains further details.

Information Management Support Council

The IMSC will provide director level guidance with Director of Information Management and Rctg Bde commanders' input to the USAREC IRM Program. The IMSC is chaired by the USAREC CofS. The IMSC charter contains further details.

information resources management

The planning, budgeting, organizing, directing,

training, promoting, controlling, and management activities associated with the burden, collection, creation, maintenance, utilization, dissemination, and disposition of information regardless of media, and includes the management of information and information related resources and systems, whether manual or automated, such as records management activities, privacy and security of records, agency sharing and dissemination of information, and acquisition and use of automatic data processing, telecommunication, and other IT.

information technology equipment

Automation and component systems created from them, regardless of use, size, capacity, or price; whether general purpose or special purpose, Government-owned or Government-leased, and includes central processing units, accessorial and auxiliary equipment, peripheral equipment, switches, routers, and other communications support electronics.

information technology equipment resources

Software or any service related to systems definition, planning, development, installation, or maintenance, including but not limited to, systems analysis, system engineering, system design, computer programming, and system documentation resulting in system hardware and/or software applications.

management information control officer

A person assigned authority to approve, disapprove, or revise proposed management information requirements within an agency in accordance with AR 335-15.

master files

A collection of specified data stored on files which are accessible via remote access.

recruiting station

A permanent location at a facility which is manned on a full-time basis by one or more recruiters for the purpose of conducting recruiting operations.

remote terminal

Computer access device located outside the computer operation center which can be interconnected to a host computer system.

requirement control symbol

A symbol assigned to a management information requirement by the management information control officer with jurisdiction to show it has been approved under AR 335-15.

substation

A permanent location utilized by one or more recruiters on a part-time (minimum 3 days per week) regular basis to conduct recruiting operations.

user identification

A unique symbol or character string that is used by an ITE system to uniquely identify a user. The

security provided by the password system does not rely entirely on secrecy of the user's ID.

user password

A series of codes needed, in addition to user ID, to gain access to a computer system. See system user documentation for determination of specific requirements for system passwords. All passwords are protected at the FOUO level or higher, as appropriate.

validation of requirements

Actions involving evaluation and acceptance of a requirement at the various command levels. Validation does not constitute approval of the requirements and will not be used as a basis for commitment of resources.