

Security

Information Systems Security Handbook

This UPDATE printing publishes a new USAREC pamphlet.

For the Commander:

STEWART K. MCGREGOR  
Colonel, GS  
Chief of Staff

Official:

ROGER H. BALABAN  
Director, Information Management

**Summary.** This pamphlet is published as a security guide for use by individuals appointed as terminal area security officers, alternate terminal area security officers, and automated information system users.

**Applicability.** This pamphlet applies to all United States Army Recruiting Command automated information systems.

**Contents** (Listed by paragraph number)

- Purpose • 1
- References • 2
- Explanation of abbreviations • 3
- Background • 4
- Scope • 5
- Responsibilities • 6
- Assistance • 7

**Appendixes**

- A. References
- B. Army Recruiting and Accession Data System
- C. Army Recruiting Command Central Computer System
- D. Automated Data Processing Equipment
- E. Information Systems Security Briefing for Users, Supervisors, and Managers of Automated Information Systems
- F. Software
- G. Viruses

**Glossary**

**1. Purpose**

This pamphlet is published as a security guide for use by individuals appointed as terminal area security officers (TASO), alternate terminal area security officers (ATASO), and automated information system (AIS) users. The responsibilities of the information systems security program manager (ISSPM), information systems security manager (ISSM), information systems security officer (ISSO), TASO, ATASO, and AIS users are defined along with the TASO, ATASO, and AIS

**Impact on New Manning System.** This pamphlet does not contain information that affects the New Manning System.

**Suggested improvements.** The proponent agency of this pamphlet is the Office of the Director of Information Management. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended

user procedures that are specific to a particular host system; points of contact for assistance and guidance; and basic automation security procedures.

**2. References**

Required and related publications and blank forms are listed in appendix A.

**3. Explanation of abbreviations**

Abbreviations used in this pamphlet are explained in the glossary.

**4. Background**

The increased use of personal computers (PC) and network interconnectivity increases the potential for unauthorized access to computer systems. Unauthorized access, whether intentional or inadvertent, increases the potential for compromise of information, destruction of data, and possible migration of viruses. To protect against these dangers the U.S. Army Information Systems Security Program (AISSP) was established to consolidate and focus Army efforts in securing information. A clearly defined structure of information systems security (ISS) personnel was established for implementing the AISSP. This pamphlet addresses AIS security as it relates to the United States Army Recruiting Command (USAREC). The USAREC ISS structure consists of the ISSPM, ISSM, ISSO, network security officer(s), TASO, and AIS users. To maintain an environment free of threats or contamination it is critical that everyone in the ISS structure understand their responsibilities and comply with security precautions and procedures in the protec-

Changes to Publications and Blank Forms) directly to HQ USAREC (RCIM-CE-OP), Fort Knox, KY 40121-2726.

**Distribution.** Distribution of this pamphlet has been made in accordance with USAREC Pam 25-30, distribution A. This pamphlet is published in the Recruiting Station Administration UPDATE.

tion of automation assets.

**5. Scope**

a. This pamphlet applies to all USAREC AIS (AIS includes stand-alone computers, small computers, word processors, multi-user computers, terminals, and networks). USAREC's Army Recruiting Command Central Computer System (ARC3S), Army Recruiting and Accession Data System (ARADS), and local unique local area network (LAN) systems are considered host systems. PC are considered automated data processing equipment (ADPE). Use and access to host systems and ADPE is restricted based on need-to-know, job relation, and mission requirements. To access these systems you must follow the procedures outlined in the applicable appendix.

- (1) Appendix B (ARADS).
- (2) Appendix C (ARC3S).
- (3) Appendix D (ADPE).

b. The Information Management Directorate has the overall responsibility for managing and maintaining the operational aspects and ensuring the security and integrity of the USAREC host and ADPE AIS. The Director of Information Management is the designated accreditation authority for USAREC-owned and/or -operated host systems and ADPE processing unclassified sensitive level information. Information Management Directorate will staff a host system project management office(s) and an ISSM for centralized management of these elements.

c. Headquarters, United States Army Recruiting Command (HQ USAREC) will appoint an ISSO and each recruiting brigade (Rctg Bde) will

\*This pamphlet supersedes USAREC Pamphlet 380-3, 1 October 1991.

dual appoint the information management officer (IMO) as the ISSO. The ISSO will serve as central point of contact for AIS issues within their organization.

## 6. Responsibilities

a. ISSPM. The ISSPM establishes, manages, and assesses the effectiveness of the ISS Program within the command.

b. ISSM. The ISSM establishes, manages, and promulgates the command's ISS Program and guidance in accordance with AR 380-5 and AR 380-19 to include developing command-unique guidance, as required. The ISSM is responsible for the security of USAREC host systems and AIS on a day-to-day basis from an administrative perspective. The ISSM develops this pamphlet and is the central coordination for preparation of security accreditation documentation for USAREC host systems.

c. ISSO.

(1) Host system ISSO. The host system ISSO is responsible for security of the host computer system on a day-to-day basis from an operational perspective. The host system ISSO ensures implementation and compliance of established Department of the Army, United States Army Information Systems Command (USAISC), and USAREC policies and procedures, develops the host system standing operating procedures (SOP), and prepares and maintains the host system AIS security accreditation. The host system ISSO serves as central point of contact for host system security issues.

(2) HQ USAREC and Rctg Bde ISSO. The HQ USAREC and Rctg Bde ISSO are responsible for security of the organization's AIS on a day-to-day basis from an operational perspective. The HQ USAREC and Rctg Bde ISSO ensure implementation and compliance of established Department of the Army, USAISC, and USAREC policies and procedures and that a TASO and ATASO are appointed as necessary (TASO is not required if all AIS is under the direct control of the ISSO). The HQ USAREC and Rctg Bde ISSO develop the organization's training and awareness program, AIS SOP, and prepare and maintain the organization's ADPE AIS security accreditation. The HQ USAREC and Rctg Bde ISSO will serve as the central point of contact for AIS security issues within their organization.

d. TASO. A TASO and ATASO will be appointed at each Rctg Bde, recruiting battalion (Rctg Bn), and HQ USAREC directorate and/or department for each terminal, workstation, or contiguous group of terminals not under the direct control of the ISSO. The TASO and ATASO will be written appointments (see fig 1) with a copy provided to the ISSO and ISSM. The TASO is the individual concerned with the security of automated systems on a day-to-day basis for an office, room, or assigned area where a terminal, group of terminals, or PC are located. The TASO and ATASO must have access to the terminal, group of terminals, or PC for which he or she is responsible for monitoring user access. The

TASO and/or ATASO will perform the following duties:

(1) Issue written instructions specifying security requirements and operating procedures.

(2) Establish each terminal user's identity, need-to-know, level of clearance, and access authorizations commensurate with the data available from that terminal.

(3) Establish procedures to restrict entry of unauthorized transactions or data.

(4) Monitor local compliance with security procedures.

(5) Assist the host system ISSO in providing system security.

(6) Report actual or suspected violations to the ISSO.

(7) Ensure that Government equipment is used to process official Government business only.

(8) Ensure users understand the necessity and procedures for changing passwords.

(9) Ensure users log-off terminals and/or PC upon departure from the work area.

(10) Provide users with instructions or procedures for protecting all printouts containing personal in nature or For Official Use Only (FOUO) data received from the host and ensure such printouts are labeled accordingly when provided to authorized individuals.

(11) Ensure users do not process classified data on USAREC AIS.

(12) Ensure that USAREC Label 19 (This Equipment Will Not Be Used to Process Classified Material) (fig 2) is attached to each AIS keyboard.

(13) Ensure that USAREC Poster 7 (When Using This Copier) is posted by each copier machine.

(14) Process requests for new user identifications (ID) in accordance with the applicable host system as identified in the appropriate appendix.

(15) Use USAREC Poster 15-R (Information Systems Security Personnel) (fig 3) to post the name and telephone number of the ISSM, ISSO, TASO, and ATASO within the terminal area. This poster will be locally reproduced on 8 1/2" x 11" paper. Colored paper may be used.

(16) Notify their ISSO if TASO or ATASO needs to be reappointed due to departure of an individual.

(17) Advise users to position terminal monitors in a manner to prevent viewing of entry features by unauthorized personnel, if possible.

(18) Inform users that sharing user ID and passwords is not authorized and anyone doing so is solely responsible for any consequences of lost data or problems.

(19) Ensure that all users, supervisors, and managers of AIS read and sign the Information Systems Security Briefing at appendix E.

(20) Conduct periodic, at least annually, inspections using USAREC Fm 1085-R (Information Systems Security Checklist) (fig 4).

e. Users. AIS users will be given host system and ADPE AIS access based on their identity, need-to-know, level of clearance, job requirements, and access authorizations commensu-

rate with the data available from that system and/or terminal. As the first line in establishing and maintaining AIS security it is crucial that the AIS user understand the following issues:

(1) Security requirements for remote terminals or PC, individual passwords, and data transmitted to and from the USAREC host system.

(2) Requirements to protect personal, Privacy Act, and FOUO information as sensitive data and the procedures to mark and/or cover sensitive data with appropriate cover sheets.

(3) Proper log-off procedures and requirements to log-off all systems prior to leaving the work area.

(4) AIS users will not share their individual user ID and passwords.

(5) The USAREC host systems and ADPE are accredited for processing unclassified sensitive data and, as such will not be utilized to transmit classified data.

(6) Procedures to report suspected and/or actual terminal security violations to the supervisor, ATASO, TASO, ISSO, or ISSM.

(7) Procedures to shutdown and report when a suspected and/or actual virus is detected.

(8) Procedures for obtaining and installing software.

(9) Ensure that USAREC Label 19 is attached to each AIS keyboard.

(10) The AIS user will consult with the TASO and/or ATASO for solving problems or assistance prior to contacting the ISSO, ISSM, or Help Desk.

f. To assist the TASO, ATASO, and AIS users, the following appendixes provide required procedures for a specific area as relates to the ISS mission:

(1) Appendix F (software).

(2) Appendix G (viruses).

## 7. Assistance

a. ISS assistance.

(1) Assistance in identifying AIS security requirements is available from HQ USAREC, Information Management Directorate, Operations and Projects Branch. The appropriate ISSO should request assistance directly from HQ USAREC (RCIM-CE-OP) at 1-800-223-3735, extension 6-0027, or HQ USAREC (RCIM-CE-OP), 1307 3rd Avenue, Fort Knox, KY 40121-2726.

(2) The TASO and/or ATASO should consult their ISSO for AIS security assistance prior to contacting HQ USAREC (RCIM-CE-OP).

b. General assistance. Hardware and software assistance is available from the Information Management Help Desk at 1-800-223-3735, extension 6-1077. Individual AIS users requiring assistance should consult with their TASO and/or ATASO for solving problems or assistance prior to contacting the ISSO, ISSM, or Help Desk.

(APPROPRIATE LETTERHEAD)

OFFICE SYMBOL

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Additional Duty Appointment/Assignment

1. Effective \_\_\_\_\_, (vice \_\_\_\_\_) you are assigned the following additional duty:

\_\_\_\_\_ Terminal Area Security Officer (TASO)

\_\_\_\_\_ Alternate Terminal Area Security Officer (ATASO)

Grade/Rank	Name (Last, First, MI)	SSN
------------	------------------------	-----

Current Unit Assignment	Telephone
-------------------------	-----------


Duty Mailing Address

2. Authority: AR 380-19.
3. Purpose: To perform duties in accordance with AR 380-19.
4. Periods: Until officially relieved or released from this appointment.
5. TASO or ATASO will serve as this activity's point of contact for all automated information systems (AIS) security-related matters.

Signature Block &  
Signature

DISTRIBUTION:  
 RCIM, ISSM  
 ISSO  
 Official Personnel File  
 Supervisor  
 Individual Concerned

Figure 1. Sample TASO and ATASO appointment

**THIS EQUIPMENT WILL NOT BE  
USED TO PROCESS CLASSIFIED  
INFORMATION!**



USAREC Label 19, 1 Jan 96

**Figure 2. Sample of a USAREC Label 19**



# INFORMATION SYSTEMS SECURITY PERSONNEL

(For use of this poster see USAREC Pam 380-5)



## INFORMATION SYSTEMS SECURITY PROGRAM MANAGER (ISSPM)

Barbara J. Wolfe, DSN 536-0650 or Commercial (502) 626-0650

## INFORMATION SYSTEMS SECURITY MANAGER (ISSM)

John W. Teegarden, DSN 536-0027 or Commercial (502) 626-0027, Facsimile 6-0912

## INFORMATION SYSTEMS SECURITY OFFICER (ISSO)

Tod Ranger, 555-3006

---

## TERMINAL AREA SECURITY OFFICER (TASO)

Alice Lloyd, 555-8008

---

## ALTERNATE TERMINAL AREA SECURITY OFFICER (ATASO)

Gerald Frost, 555-6686

---

### NOTES

1. The TASO or ATASO should add the names and telephone numbers of the ISSO, TASO, and ATASO and display this poster in the TASO and ATASO area of responsibility for automated information system (AIS) security.
2. TASO and ATASO appointments must be submitted via facsimile to the ISSM listed above.
3. Individuals experiencing any known or suspected security violations, viruses, malfunctions, or other problems with an AIS or automated data processing equipment (ADPE) should notify their TASO or ATASO.

USAREC Poster 15-R, 1 Jan 96

Figure 3. Sample of a completed USAREC Poster 15-R

**INFORMATION SYSTEMS SECURITY CHECKLIST**

(For use of this form see USAREC Pam 380-5)

	YES	NO	N/A
<b>1. TASO AND ATASO:</b>			
a. Has a terminal area security officer (TASO) and alternate terminal area security officer (ATASO) been appointed for each interconnected computer and terminal, or group of contiguous terminals?	✓		
b. Is the TASO and ATASO properly appointed in writing? If so, attach letter of appointment to this document. If not, obtain letter of appointment and attach to this document.	✓		
c. Does the TASO and ATASO have a copy of AR 380-19?	✓		
d. Does the TASO and ATASO ensure that instructions specifying security requirements and operating procedures are available for each terminal area he or she is responsible for?	✓		
e. Has the TASO and ATASO ensured that each terminal user's identification (ID), need-to-know, level of clearance, and access authorization is established commensurate with the data available from that terminal?	✓		
f. Does the TASO and ATASO manage the control and dissemination of user and file ID numbers and default passwords?	✓		
g. Is the TASO and ATASO aware of who accesses the terminal(s) and what outputs are printed from the terminals?	✓		
h. Does the TASO and ATASO mark, handle, process, and store Privacy Act and For Official Use Only (FOUO) data, printouts, and diskettes accordingly?	✓		
i. Has the TASO and ATASO implemented controls to prevent entry of unauthorized transactions of data (e.g., classified data over unsecured data transmission lines)?	✓		
j. Does the TASO and ATASO check and ensure that remote terminals are available only to a authorized individuals?	✓		
k. Does the TASO and ATASO conduct periodic training in regards to existing regulations and procedures governing the proper usage of the terminal and sign-on and sign-off procedures?	✓		
l. Does the TASO and ATASO check and ensure that terminal boards and other communications equipment associated with the teleprocessing computer system are located in locked rooms where access has been strictly controlled?	✓		
m. Where possible, is the TASO's and ATASO's terminal located to assure privacy and prevent viewing of entry features by unauthorized individuals?	✓		
n. Has the TASO and ATASO changed the default to a personal password?	✓		
o. Is the TASO's and ATASO's personal password known only by the user?	✓		
p. Does the TASO and ATASO enforce local compliance with security operating procedures for that terminal?	✓		
q. Is the TASO and ATASO performing all possible actions to assist the host system information systems security officer (ISSO) in ensuring that overall system security is being affected?	✓		
<b>2. PHYSICAL AND ENVIRONMENTAL:</b>			
a. Are positive physical access controls established to prevent unauthorized entry into the area where computer equipment is located?	✓		
b. Are the buildings or facilities selected to house computer equipment sufficient structural integrity so as to provide, or capable of being made, to provide effective physical security at a reasonable cost?	✓		
c. Do the physical characteristics of the location selected to house the automated system support the establishment of an effective physical security system at the facility?	✓		
d. Is the computer area secured upon completion of the duty day or at any time the facility is unmanned?	✓		
USAREC Fm 1085-R, 1 Jan 96 (This form replaces USAREC Fm 1039 which is obsolete)			

**Figure 4. Sample of a completed USAREC Fm 1085-R**

	YES	NO	N/A
e. Is strict accountability maintained over keys, combinations, or identification numbers which permit access to the facility?	✓		
f. Is there an organization or activity representative present during janitorial cleaning operations?		✓	
g. Are areas containing remote terminals secured during and after hours consistent with the level of information accessed by the terminal?	✓		
h. Are positive administrative safeguards being implemented to ensure that only authorized individuals are permitted to utilize remote terminal equipment capable of accessing the computer systems?	✓		
i. Has adequate fire protection for mission-essential automated systems been achieved through a combination of minimizing the exposure to fire damage by assuring prompt detection and by providing adequate means to extinguish the fire?	✓		
j. Have conflicts between security and fire safety requirements been brought to the attention of the commander?	✓		
k. Within the facility, have good housekeeping and operating procedures been prerequisites to maintaining a noncombustible environment?	✓		
l. Have the use of tobacco products, eating, and drinking been strictly prohibited in the areas where automated data processing equipment is being used?	✓		
m. Has a minimum degree of fire protection, primarily being handheld extinguishing equipment, been implemented with additional protection provided by an area extinguishing system or systems, as appropriate?	✓		
n. Is fire extinguishing equipment immediately available for use in controlling fires in a computer equipment area?	✓		
o. Are a sufficient number of carbon dioxide (CO2) extinguishers available for use in case of nonelectrical fires and installed in accordance with NFPA Code 10?	✓		
p. Are water type fire extinguishers also available for use on nonelectrical fires?		✓	
q. Are handheld extinguishers marked to indicate the type of fire for which they are intended?	✓		
r. Have commanders ensured that orientation and training classes are held to enable personnel who work around computer equipment to become familiar with facility fire equipment (emergency) and procedures?	✓		
s. Are cost effective security measures implemented to ensure that sensitive information is properly protected at all times?	✓		
t. Is the environmental protection consistent with the equipment manufacturer's recommendation?	✓		
u. Is fire protection achieved by the installation of local smoke alarms and portable extinguishing equipment?	✓		
v. Has the commander at each facility assured that adequate procedures have been established to obtain firefighting assistance from the local fire department?	✓		
w. Is office equipment properly safeguarded?	✓		
x. Are expendable supplies properly safeguarded?	✓		
y. Are communication-electronic items provided adequate security?	✓		
z. Are adequate inspections being made to determine the effectiveness of the Information Security Program both within activities and in subordinate elements?	✓		
aa. Are information and material afforded protection commensurate with the level of classification assigned?	✓		
ab. Are material and diskettes properly marked with the overall classification (FOUO, Privacy Act)?	✓		
ac. Are FOUO material and diskettes being properly safeguarded?	✓		
ad. Are FOUO material and diskettes being properly destroyed?	✓		

Figure 4. Sample of a completed USAREC Fm 1085-R (Continued)

	YES	NO	N/A
<b>3. PERSONNEL SECURITY:</b>			
a. Have all automation personnel been provided an appropriate security briefing upon arrival at the organization or activity before beginning their assigned duties?	✓		
b. Do security briefings include information on AR 380-19:			
(1) Duties individual is expected to perform?	✓		
(2) Local security environment?	✓		
(3) Computer hardware and software?	✓		
(4) Individual security responsibilities?	✓		
c. Has a continuing security education program been established?	✓		
d. Where required, are users checked to ensure that they have undergone a satisfactory security background check before issuance of a user ID and password?	✓		
e. Are user ID issued on a need-to-know, job relation, and mission requirements basis?	✓		
f. Are user ID promptly deleted for users that no longer require access due to change in operational requirements or departure?	✓		
<b>4. COMMUNICATIONS SECURITY AND TERMINAL ACCESS:</b>			
a. Is the responsibility for issuance and control of all system's user ID handled by the TASO or ATASO?	✓		
b. After generation, are systems user ID handled and stored at the level of FOUO?	✓		
c. At the time of user ID and password issuance, are users briefed on password protection, methods to safeguard, unauthorized use, and to inform the TASO or ATASO of misuse?	✓		
d. Are personal passwords changed periodically?	✓		
e. Are all cases of actual or suspected compromise of a given password investigated immediately by the TASO or ATASO and reported to the ISSO?	✓		
<b>5. SOFTWARE:</b>			
a. Are there provisions that ensure all software is accounted for?	✓		
b. Is software being used within the manufacturer's licensing agreement?	✓		
c. Are operators informed of requirements and procedures to protect the integrity of software manufacturer's licensing agreement?	✓		
d. Are the master copy diskettes write protected, properly stored, safeguarded, and never used for actual production operations?	✓		
e. Is the "latest" version of antiviral software being employed?	✓		
<b>6. PROCEDURAL:</b>			
a. Does the TASO and ATASO maintain a current host system user access roster of all personnel authorized access to the system?	✓		
b. Does the system user access roster contain the name, grade, organization, user ID code, and function applicable?	✓		
c. Are interval procedures for the following established:			
(1) Fire evacuation?	✓		
(2) Activating fire alarms?	✓		
(3) Fire and police help?	✓		

Figure 4. Sample of a completed USAREC Fm 1085-R (Continued)

	YES	NO	NA
(4) Safety do's and don'ts:			
(a) For operating equipment?	✓		
(b) Smoking, eating, and drinking areas?	✓		
(c) Site cleanliness?	✓		
d. Are there policies and procedures for positive control of portable terminals to prevent their theft and misuse?	✓		
e. Are personal passwords known by only one user?	✓		
f. Are passwords changed periodically?	✓		
g. Have procedures been established for the continuing protection of automated data processing files, application and system software, and the system documentation?	✓		
h. Is local compliance with security operating procedures for that terminal site being enforced?	✓		
i. Are all possible actions to assist the host system ISSO in ensuring overall system security being effected?	✓		
<b>7. RISK MANAGEMENT:</b>			
a. Has a risk management assessment been performed?	✓		
b. Is the review of identified risks and determining appropriate countermeasures a function of top level management?	✓		
<b>8. PRIVACY SAFEGUARDS FOR AUTOMATED SYSTEMS:</b>			
a. Does the automated data processing system(s) process or store any Privacy Act information?	✓		
b. Are Privacy Act waste products being properly disposed of?	✓		
c. Are Privacy Act output products and storage media labeled FOUO - PRIVACY ACT DATA?	✓		
<b>9. REQUIRED DIRECTIVES:</b>			
a. Does the command have the following publications on hand and current:			
(1) AR 25-1 (The Army Information Resources Management Program)?	✓		
(2) AR 340-21 (The Army Privacy Program)?	✓		
(3) AR 380-5 (Department of the Army Information Security Program)?	✓		
(4) AR 380-19 (Information Systems Security)?	✓		
(5) AR 380-53 (Communications Security Monitoring)?	✓		
(6) AR 380-67 (Department of the Army Personnel Security Program)?	✓		
(7) AR 710-2 (Inventory Management Supply Policy Below the Wholesale Level)?	✓		
(8) DA Pam 710-2-1 (Using Unit Supply System (Manual Procedures))?	✓		
b. Does the command have on hand and use:			
(1) USAREC Label 19?	✓		
(2) USAREC Poster 7?	✓		
(3) USAREC Poster 15-R?	✓		
(4) DD Form 2056?	✓		

Figure 4. Sample of a completed USAREC Fm 1085-R (Continued)



**Appendix A  
References**

**Section I  
Related Publications**

**AR 25-1**

The Army Information Resources Management Program.

**AR 25-55**

The Department of the Army Freedom of Information Act Program.

**AR 340-21**

The Army Privacy Program.

**AR 380-5**

Department of the Army Information Security Program.

**AR 380-19**

Information Systems Security.

**AR 380-53**

Communications Security Monitoring.

**AR 380-67**

The Department of the Army Personnel Security Program.

**AR 710-2**

Inventory Management Supply Policy Below the Wholesale Level.

**DA Pam 710-2-1**

Using Unit Supply System (Manual Procedures).

**USAREC Reg 25-1**

Information Resources Management Program.

**Section II  
Required Forms**

**USAREC Fm 1085-R**

Information Systems Security Checklist.

**USAREC Fm 1086-R**

ARADS User Access Request (Headquarters and Staff Elements).

**USAREC Fm 1087-R**

ARADS User Access Request (Brigade and Battalion).

**USAREC Fm 1088-R**

User ID Receipt.

**USAREC Label 19**

This Equipment Will Not Be Used to Process Classified Material.

**USAREC Poster 15-R**

Information Systems Security Personnel.

**Section III  
Related Forms**

**DA Label 87**

For Official Use Only Cover Sheet.

**DD Form 2056**

Telephone Monitoring Notification Decal.

**USAREC Poster 7**

When Using This Copier.

## Appendix B Army Recruiting and Accession Data System

### B-1. Purpose

The purpose of this appendix is to identify duties and responsibilities of the TASO and AIS user that are specific for the operational security of ARADS.

### B-2. Scope

Each activity or organization maintaining an ARADS terminal(s) will appoint a TASO and ATASO for each terminal or contiguous group of terminals not under the direct control of an ISSO. Written appointments for TASO and ATASO will be prepared (sample at fig 1) and forwarded to HQ USAREC (RCIM-CE-OP) or submitted via facsimile (502) 626-0912.

### B-3. ARADS duties of TASO

AR 380-19, paragraph 1-6d(5), USAREC Reg 25-1, and this pamphlet identify duties of the TASO.

NOTE: Wherever reference is made to TASO the same duties and responsibilities apply to the ATASO.

### B-4. ARADS responsibilities of the TASO

The TASO is responsible for the day-to-day operational security of an activity's or organization's ARADS. The TASO and ATASO:

- a. Is required to possess an ARADS user ID to perform their duties and responsibilities associated with ARADS.
- b. Identifies ARADS users based on need-to-know, job relation, and mission requirements.
- c. Obtains USAREC Fm 1086-R (ARADS User Access Request (Headquarters and Staff Elements)) (fig B-1) or USAREC Fm 1087-R (ARADS User Access Request (Brigade and Battalion)) (fig B-2) as appropriate, to enter new users into ARADS.
- d. Uses USAREC Fm 1088-R (User ID Receipt) (fig B-3) to issue the individual's user ID.
- e. Promptly deletes users who no longer require access due to change in operational requirements or departure.
- f. Reports hardware terminal problems to the local ISSO or IMO.
- g. Reports possible or actual terminal security violations to the ISSO.
- h. Informs all ARADS users of their duties (see para B-5).

### B-5. Responsibilities of ARADS users

The ARADS user's access is based on need-to-know, job relation, and mission requirements. The ARADS user is responsible for the day-to-day operational and functional security of an individual ARADS ID. In addition to the responsibilities identified in paragraph 6e, the ARADS user will:

- a. Adhere to the security requirements for remote terminals, individual passwords, site ID codes, perishable passwords, and data transmitted to and from ARADS.
- b. Handle all information from the ARADS

data bases containing personal information as highly sensitive data and comply with the provisions of the Privacy Act of 1974, AR 340-21, and as follows:

- (1) Personal information is guarded in the same way as FOUO.
- (2) Data transferred to diskette governed by the Privacy Act and/or FOUO will have the diskette marked FOUO and the diskette will be treated in the same manner as "hard copy" FOUO material.
  - c. Comply with proper sign-on and sign-off procedures.
  - d. Users experiencing a problem, either hardware, software, or system on a terminal should contact their TASO or ATASO. Problems which cannot be corrected by the TASO or ATASO should be referred to the USAREC ARADS Hot Line at DSN 464-2141 or USAREC Toll-Free Number 1-800-223-3735, extension 4-2141.
  - e. Each remote terminal will be active only when an authorized terminal user is present and using the equipment. Any violation of this procedure is a security violation. Prior to departing, each user must properly sign-off the terminal and ensure access cannot be gained without initiating proper sign-on procedures.
  - f. Suspected or actual terminal security violations will be reported to the appropriate TASO, who in turn will contact the ISSO. Security problems which cannot or are not corrected by the TASO, ATASO, or ISSO should be referred to HQ USAREC (RCIM-CE-OP) at DSN 536-0027 or USAREC Toll-Free Number 1-800-223-3735, extension 6-0027.
  - g. New users are required to apply to the TASO for user ID issue and initial AIS security briefing.
  - h. Users will not smoke, eat, or drink at a terminal or workstation.
  - i. Personal passwords are not to be given to unauthorized users or left out in plain view. Authorized users will not allow another individual to use his or her unique user ID and password. An attempt to access or actual access to the mainframe by posing as an authorized user (with their user ID) is termed masquerading or mimicking and is a security violation.
  - j. Old passwords and sensitive information (FOUO) should be destroyed by tearing, shredding, or mutilating to render personal data unrecognizable and beyond reconstruction in accordance with AR 25-55, chapter 4.
  - k. Security violations (unauthorized user, passwords not stored as FOUO, etc.) and any loss or theft of ADPE property must be reported to the TASO.
    - l. Personal passwords should be changed every 90 days or whenever the user believes their password may have been compromised. To change an ARADS password of TOYBOX to CAPGUN:
      - (1) Log-on using the current password (TOYBOX).
      - (2) At the OK prompt type CPW (OLD PASSWORD) and press ENTER (i.e., CPW toybox).
      - (3) Now type the new password CAPGUN

and press ENTER (i.e., capgun).

(4) The system will then prompt you to retype the new password to confirm.

(5) The new password will then be operative at the next log-on. Passwords are a minimum of six characters and a maximum of eight characters long.

### B-6. Procedures for issuing user ID

a. The commander or supervisor uses USAREC Fm 1086-R or USAREC Fm 1087-R, as appropriate, to request a user ID be assigned based on the individual's need-to-know, job relation, and mission requirements.

b. The TASO has the user complete USAREC Fm 1088-R, items 1 through 5.

c. The TASO completes items 6 and 7 and assigns the user ID(s). The ARADS user ID (does not apply to recruiting station users) is assigned as follows:

- (1) The first digit is the individual's last name initial.
- (2) The next nine digits are the individual's social security number (SSN).
- (3) The last digit(s) are the individual's recruiting station identification (RSID).
- (4) See figure B-4 for assigning ARADS user ID.

d. The TASO has the individual date and initial beside the user ID to acknowledge its receipt and has the user read, sign, and date the statement at the bottom of the form.

NOTE: The information is obtained on USAREC Fm 1088-R under the Privacy Act of 1974 for the purpose of obtaining user ID and password to access a USAREC host AIS. This form and/or any reuse of the information garnered from it to obtain a user ID will be treated as FOUO.

e. The TASO verifies particular access requirements for the individual and that the individual has successfully undergone a security background check.

f. The TASO uses ARADS User-Reg module to enter the individual for access to ARADS.

NOTE: Individual must be entered in the Command Integrated Management System (CIMS) before they can be entered in ARADS. Attempts to enter individuals into ARADS not in CIMS will result in "INDIVIDUAL NOT IN CIMS-CALL S-1 OFF" error message.

g. The TASO monitors User-Reg and View User Access Request Status modules for "REQUESTED ACTION SENT, FULL APPROVAL GIVEN, AWAITING ACTION" message. This message signifies that the individual has been successfully entered for ARADS access.

h. The TASO notifies the individuals that they have access to ARADS and ensures that they know how to perform initial log-on and change their password. When the individual conducts an initial log-on the system automatically clears the above message.

NOTE: Individuals observed accessing ARADS without the above message clearing have not been properly entered or are using another individual's user ID and password.

**B-7. Procedures for deleting user ID**

a. When individuals having access no longer require such access, due to change in operational requirements or departure, the user's ID will be deleted from the system.

b. The commander or supervisor requests the user ID be deleted as no longer requiring access. The TASO uses ARADS User-Reg module to delete the individual for access to ARADS.

**B-8. Procedures for correcting user ID data**

a. Job transfer within unit. The TASO uses ARADS User-Reg module to edit the individual's access to ARADS.

b. Unit transfer within the Rctg Bn (with different RSID).

(1) Transfer must be entered in the S1 CIMS.

(2) The TASO uses ARADS User-Reg module to delete the individual for access to ARADS.

(3) The TASO uses ARADS User-Reg module to add the individual for access to ARADS (after individual has been added the new RSID should be reflected).

**B-9. Assistance**

a. ISS assistance.

(1) Assistance in identifying AIS security requirements is available from HQ USAREC (RCIM-CE-OP). The appropriate ISSO should request assistance directly from HQ USAREC (RCIM-CE-OP) at 1-800-223-3735, extension 6-0027.

(2) The TASO and/or ATASO should consult their ISSO for AIS security assistance prior to contacting HQ USAREC (RCIM-CE-OP).

b. General assistance. Hardware and software assistance is available from the ARADS Help Desk at 1-800-223-3735, extension 4-2141. Individual AIS users requiring assistance should consult with their TASO and/or ATASO for solving problems or assistance prior to contacting the ISSO, ISSM, or Help Desk.

**ARADS USER ACCESS REQUEST (Headquarters and Staff Elements)**

(For use of this form see USAREC Pam 380-5)

**Information Required By the Privacy Act of 1974**

**Authority:** 5 USC 522A, Public Law 93-579, AR 340-21, and AR 380-19.

**Principal Purpose:** Used to identify and authorize AIS users and assign user identification (ID) codes required to access USAREC host systems.

**Routine Uses:** To assign individual's user ID code(s) and add user ID for access to USAREC host system(s).

**Disclosure:** Voluntary. Failure to furnish the information requested will result in denial of user ID(s) issuance and access to USAREC host system.

**User ID are issued to individuals based on need-to-know, job relation, and mission requirements.**

**Print or Type User Data**

1. NAME: Jane L. Doe 2. GRADE/RANK: GS-07 3. SSN: 123-45-6789  
 4. ORGANIZATION: Personnel Directorate 5. DUTY POSITION: Admin Clerk  
 6. DUTY TELEPHONE: COMMERCIAL: (999) 555-5551 DSN: 554-5551 7. DATE: 20 Dec 95

**HEADQUARTERS AND STAFF ELEMENTS**

RECRUITING	HUMAN RESOURCES	ADVERTISING AND SALES
<input type="checkbox"/> HQ-RO-ADMIN	<input checked="" type="checkbox"/> HQ-AGR	<input type="checkbox"/> HQ-BUDGET & ACCOUNTING
<input type="checkbox"/> HQ-RO-E	<input checked="" type="checkbox"/> HQ-AWARDS	<input type="checkbox"/> HQ-DISTRIBUTION
<input type="checkbox"/> HQ-RO-GC	<input type="checkbox"/> HQ-COMDT	<input type="checkbox"/> HQ-PROCUREMENT
<input type="checkbox"/> HQ-RO-OWNRS	<input type="checkbox"/> HQ-CPO	<input type="checkbox"/> HQ-LOCAL MEDIA PAYMENT
<input type="checkbox"/> HQ-RO-PP	<input type="checkbox"/> HQ-DRUG	<input type="checkbox"/> HQ-MEDIA
<input type="checkbox"/> HQ-RO-S	<input checked="" type="checkbox"/> HQ-EMB	<input type="checkbox"/> HQ-PRINT
<input type="checkbox"/> HQ-RO-T	<input type="checkbox"/> HQ-OMD	<input type="checkbox"/> HQ-PRODUCTION CONTROL
<input type="checkbox"/> FT JACKSON SCH STAFF	<input type="checkbox"/> HQ-PB	<input type="checkbox"/> HQ-PROJECT OFFICER
<input type="checkbox"/> FT JACKSON INSTR/STU	<input checked="" type="checkbox"/> HQ-SECURITY	<input type="checkbox"/> HQ-RISC PERSONNEL
	<input type="checkbox"/> HQ-STATS	<input type="checkbox"/> HQ-SALES PROMOTION
	<input type="checkbox"/> SCHOOL LIAISON	<input type="checkbox"/> HQ-TRAVEL

**FINANCE AND LOGISTICS**

<input type="checkbox"/> HQ-CH, LOG DIV	<input type="checkbox"/> HQ-LOGISTICS SGT	<input type="checkbox"/> HQ-RML ARADS POC
<input type="checkbox"/> HQ-CH & SEC FAC & SVC BR	<input type="checkbox"/> HQ-CONTRACT SPEC	<input type="checkbox"/> HQ-MICO
<input type="checkbox"/> HQ-REALTY SPEC	<input type="checkbox"/> HQ-FORCE STR DIV CH	<input type="checkbox"/> HQ-HQ COMDT
<input type="checkbox"/> HQ-LOG MGT SPEC	<input type="checkbox"/> HQ-REQ & ORG	<input type="checkbox"/> HQ-HQ TRUCKMASTER
<input type="checkbox"/> HQ-CH, SUP & VEH BT	<input type="checkbox"/> HQ-PROG & TDA BR	<input type="checkbox"/> HQ-HQ PBO
<input type="checkbox"/> HQ-LOG SPEC (EQUIPMENT)	<input type="checkbox"/> HQ-MICO LIN (RML)	<input type="checkbox"/> HQ-HQ SUPPLY
<input type="checkbox"/> HQ-LOG SPEC (VEHICLES)	<input type="checkbox"/> HQ-BUDGET	<input type="checkbox"/> HQ-HQ UNIT HOUSING REP

**REQUESTING COMMANDER OR SUPERVISOR**

1. NAME: Alec C. Strong 2. GRADE/RANK: GS-13 3. TELEPHONE: 555-5651  
 4. SIGNATURE: /signed/ 5. DATE: 20 Dec 95

USAREC Fm 1086-R, 1 Jan 96

**Figure B-1. Sample of a completed USAREC Fm 1086-R**

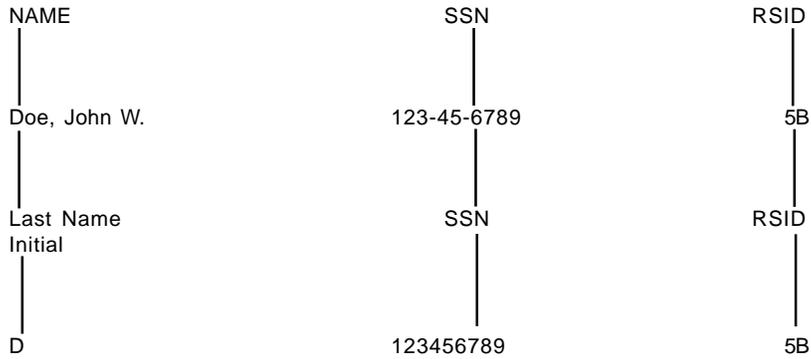




User ID are assigned in ARADS as follows:

1. The first digit is the individual's last name initial.
2. The next nine digits are the individual's SSN.
3. The last digit(s) is the individual's RSID.

Example: John W. Doe, SSN 123-45-6789, RSID 5B, would be assigned user ID D1234567895B in the following manner:



**Figure B-4. Assigning ARADS user ID**

## Appendix C

### Army Recruiting Command Central Computer System

#### C-1. Purpose

The purpose of this appendix is to identify duties and responsibilities of the TASO and AIS users that are specific for the operational security of the ARC3S.

#### C-2. Scope

Each activity or organization maintaining an ARC3S account(s) will appoint a TASO and ATASO for each terminal or contiguous group of terminals not under the direct control of an ISSO. Written appointments for TASO and ATASO will be prepared (sample at fig 1) and forwarded to HQ USAREC (RCIM-CE-OP) or submitted via facsimile (502) 626-0912.

#### C-3. ARC3S duties of TASO

AR 380-19, paragraph 1-6d(5), USAREC Reg 25-1, and this pamphlet identify duties of the TASO.

NOTE: Wherever reference is made to TASO the same duties and responsibilities apply to the ATASO.

#### C-4. ARC3S responsibilities of TASO

The TASO is the individual responsible for the day-to-day operational security of an activity's or organization's ARC3S account(s). In addition to the responsibilities identified in paragraph 6d, the TASO and ATASO:

- a. Is not required to possess an ARC3S user ID to perform their duties and responsibilities associated with the ARC3S.
- b. Secures and maintains the default password for the activity's or organization's ARC3S account(s).
- c. Identifies ARC3S users based on need-to-know, job relation, and mission requirements.
- d. Uses USAREC Fm 1088-R (fig B-3) to assign user ID and processing ARC3S user access.
- e. Performs initial log-on for new users and password resets.
- f. Reports hardware terminal problems to the local ISSO or IMO.
- g. Reports possible or actual terminal security violations to the ISSO.
- h. Informs all ARC3S users of their duties (see para C-5).

#### C-5. Responsibilities of ARC3S users

The ARC3S user's access is based on need-to-know, job relation, and mission requirements. The ARC3S user is responsible for the day-to-day operational and functional security of an individual ARC3S ID. In addition to the responsibilities identified in paragraph 6e, the ARC3S user will:

- a. Adhere to the security requirements for remote terminals, individual passwords, site ID codes, perishable passwords, and data transmit-

ted to and from the ARC3S.

b. Handle all information from ARC3S data bases containing personal information as highly sensitive data and comply with the provisions of the Privacy Act of 1974, AR 340-21, and as follows:

- (1) Personal information is guarded in the same way as FOUO.
- (2) Data transferred to diskette governed by the Privacy Act and/or FOUO will have the diskette marked FOUO and the diskette will be treated in the same manner as "hard copy" FOUO material.

c. Comply with proper sign-on and sign-off procedures. Users will always issue the following commands to sign-off:

- (1) @fin = finishes run.
- (2) \$\$close = closes out account.
- (3) \$\$off = signs off system.

d. Users experiencing a problem, either hardware, software, or system on an ARC3S terminal should contact their TASO or ATASO. Problems which cannot be corrected by the TASO or ATASO should be referred to the Information Management Help Desk at DSN 536-1077 or USAREC Toll-Free Number 1-800-223-3735, extension 6-1077.

e. Each remote terminal will be active only when an authorized terminal user is present and using the equipment. Any violation of this procedure is a security violation. Prior to departing, each user must properly sign-off the terminal and ensure access cannot be gained without initiating proper sign-on procedures.

f. Suspected or actual terminal security violations will be reported to the appropriate TASO, who in turn will contact the ISSO. Security problems which cannot or are not corrected by the TASO, ATASO, or ISSO should be referred to HQ USAREC (RCIM-CE-OP) at DSN 536-0027 or USAREC Toll-Free Number 1-800-223-3735, extension 6-0027.

g. New users are required to apply to the TASO for user ID issue and initial security briefing.

h. Users will not smoke, eat, or drink at a terminal or workstation.

i. Personal passwords are not to be given to unauthorized users or left out in plain view. Authorized users will not allow another individual to use his or her unique user ID and password. Any attempt to access or actual access to the mainframe by posing as an authorized user (with their user ID) is termed masquerading or mimicking and is a security violation.

j. Old passwords and sensitive information (FOUO) should be destroyed by tearing, shredding, or mutilating to render personal data unrecognizable and beyond reconstruction in accordance with AR 25-55, chapter 4.

k. Security violations (unauthorized user, passwords not stored as FOUO, etc.) and any loss or theft of automated data processing property must be reported to the TASO.

- l. Personal passwords will be changed every

90 days or whenever the user believes their password may have been compromised. To change an ARC3S password of TOYBOX to CAPGUN:

(1) Log-on using the current password (TOYBOX).

(2) Enter @@passwd (OLD PASSWORD)/(NEW PASSWORD) (i.e., @@passwd toybox/capgun).

(3) Press return (transmit). The system will respond "PASSWORD REPLACED."

(4) The new password will then be operative at the next log-on. The maximum length for the password is six characters. Passwords over six characters will be truncated by the system.

#### C-6. Procedures for issuing user ID

a. The commander or supervisor requests a user ID be assigned based on the individual's need-to-know, job relation, and mission requirements.

b. The TASO has the user complete USAREC Fm 1088-R, items 1 through 5.

c. The TASO completes items 6 and 7 and assigns the user ID(s). The ARC3S six-digit user ID is assigned as follows:

(1) The first two digits are the RSID (department ID for HQ USAREC staff elements).

(2) The third digit is the individual's last name initial.

(3) The fourth digit is the individual's first name initial.

(4) The last two digits are the last two digits of the individual's SSN.

(5) See figure C-1 for an example of how to assign an ARC3S user ID.

d. The TASO has the user date and initial beside the user ID to acknowledge their receipt and has the user read, sign, and date the statement at the bottom of the form.

NOTE: The information is obtained on USAREC Fm 1088-R under Privacy Act of 1974 for the purpose of obtaining user ID and password to access a USAREC host AIS. This form and/or any reuse of the information garnered from it to obtain a user ID will be treated as FOUO.

e. The TASO verifies particular access requirements for the individual and that the individual has successfully undergone a security background check.

f. The TASO submits an ARC3S user ID request to HQ USAREC (RCIM-CE-OP) in one of the following manners:

(1) Submit the USAREC Fm 1088-R via facsimile, commercial (502) 626-0912 or DSN 536-0912.

(2) Consolidate the pertinent data (see example at fig C-2) and submit via facsimile to the telephone number in (1) above.

NOTE: When submitting multiple requests (four or more) via facsimile this is the recommended method to reduce line transmission time.

(3) Consolidate the pertinent data (see example at fig C-2) and submit via cc:mail to address ARC3S USER-REQUEST with request receipt.

NOTE: This is the recommended method to submit ARC3S requests for individuals with cc:mail access.

g. With the user present, the TASO uses the default password and conducts the initial log-on for the user ID. If the log-on is successful the system will transmit a "password expired, enter new password" message. The TASO allows the user to change their password at this time and the system should respond with "password replaced." The maximum length for the password is six characters.

NOTE 1: The TASO should secure the default password and never share it with anyone other than the ATASO.

NOTE 2: It normally requires 1 working day to process a request to add a user ID. The TASO should wait 24 hours (the next working day) from the time they transmitted the request, excluding weekends and holidays, before attempting to log-on the user.

h. When an "invalid user ID or password" message is received while attempting an initial log-on the TASO should wait an additional 24 hours (a second working day) before attempting again. Should the TASO be unable to conduct the initial log-on after 48 hours (2 working days) from the time they transmitted the request, excluding weekends and holidays, they should send a cc:mail message to ARC3S USER-REQUEST or contact HQ USAREC (RCIM-CE-OP)

at 1-800-223-3735, extension 6-0027.

### C-7. Procedures for deleting user ID

a. When individuals having access no longer require such access, due to change in operational requirements or departure, the user's ID will be deleted from the system.

b. The TASO submits a request to delete a user ID to HQ USAREC (RCIM-CE-OP) in one of the following manners:

(1) Place the user ID data to be deleted on plain bond paper (see example at fig C-3) and transmit via facsimile, commercial (502) 626-0912 or DSN 536-0912.

(2) Format a cc:mail message (see example at fig C-3) and transmit to cc:mail address ARC3S USER-REQUEST.

### C-8. Procedures for correcting user ID data

a. The TASO will receive an ARC3S USER-ID INFORMATION REPORT from HQ USAREC each quarter. The TASO will review the report for any additions, deletions, and/or corrections that may be required.

b. Additions and deletions will be processed per the requirements of paragraphs C-6 and C-7. NOTE: Additions, deletions, and/or corrections may be consolidated on plain bond paper (see example at fig C-4) and transmitted via facsimile, commercial (502) 626-0912 or DSN 536-0912 or cc:mail to ARC3S USER-REQUEST.

c. Corrections will be submitted as follows:

(1) Place the user ID data to be corrected on plain bond paper (see example at fig C-5) and transmit via facsimile, commercial (502) 626-0912 or DSN 536-0912.

(2) Format a cc:mail message (see example at fig C-5) and transmit to cc:mail address ARC3S USER-REQUEST.

NOTE: Corrections should be reflected on the next quarterly report.

### C-9. Assistance

a. ISS assistance.

(1) Assistance in identifying AIS security requirements is available from HQ USAREC (RCIM-CE-OP). The appropriate ISSO should request assistance directly from HQ USAREC (RCIM-CE-OP) at 1-800-223-3735, extension 6-0027.

(2) The TASO and/or ATASO should consult their ISSO for AIS security assistance prior to contacting HQ USAREC (RCIM-CE-OP).

b. General assistance. Hardware and software assistance is available from the Information Management Help Desk at 1-800-223-3735, extension 6-1077. Individual AIS users requiring assistance should consult with their TASO and/or ATASO for solving problems or assistance.

User ID are assigned in the ARC3S as follows:

1. The first two digits are the RSID.
2. The third digit is the individual's last name initial.
3. The fourth digit is the individual's first name initial.
4. The last two digits are the last two digits of the individual's SSN.

Example: John W. Doe, SSN 123-45-6789, RSID 5B, ARC3S account number 19005B would be assigned user ID 5BDJ89 in the following manner:

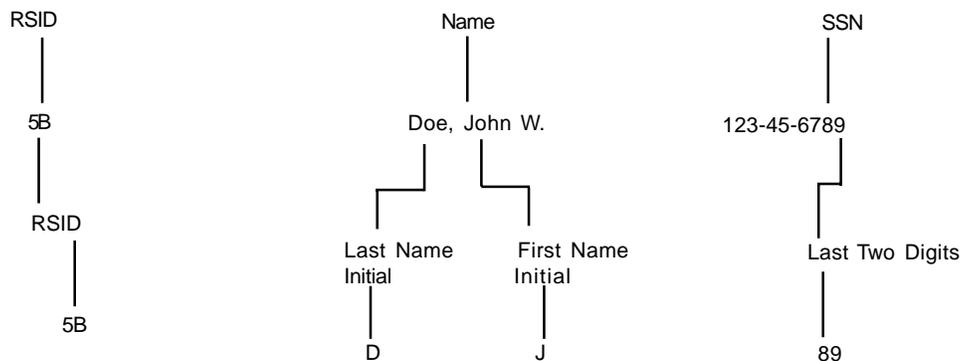


Figure C-1. Example of assigning an ARC3S user ID

Account number: 19005Z  
Account name: Mesotron Recruiting BN  
TASO: CPT Artiste N. Lister  
Effective date: Immediately

Request the following be added to the ARC3S data base.

USER ID	NAME	GRADE	SSN
5ZSJ89	SMITH, JANE L.	SFC	123-45-6789
5ZDJ21	DOE, JOHN K.	GS-04	987-65-4321

Lotta C. Curity  
CPT, IN  
ATASO

**Figure C-2. Add format for bond paper facsimile or cc:mail submission**

Account number: 19005Z  
Account name: Mesotron Recruiting BN  
TASO: CPT Artiste N. Lister  
Effective date: Immediately

Request the following be deleted from the ARC3S data base.

USER ID	NAME	GRADE	SSN
5ZSJ89	SMITH, JANE L.	SFC	123-45-6789
5ZDJ21	DOE, JOHN K.	GS-04	987-65-4321

Lotta C. Curity  
CPT, IN  
ATASO

**Figure C-3. Delete format for bond paper facsimile or cc:mail submission**

Account number: 19005Z  
 Account name: Mesotron Recruiting BN  
 TASO: CPT Artiste N. Lister  
 Effective date: Immediately

Request that the following be added to the ARC3S data base.

USER ID	NAME	GRADE	SSN
5ZSJ89	WILSON, ROBERTA J.	MSG	231-45-6789
5ZDJ21	DOE, JANE A.	GS-04	789-65-4321

Request that the following be deleted from the ARC3S data base.

USER ID	NAME	GRADE	SSN
5ZSJ89	BROWN, MICHAEL E.	CPT	321-45-6789
5ZDJ21	DOE, JOHN K.	GS-04	897-65-4321

Request the following corrections to the ARC3S data base.

USER ID	NAME	GRADE	SSN
5ZSJ89	SMITH, JANE L.	SFC	123-45-6789
	SMITHE, JANE L.		
5ZDJ21	JONES, THOMAS K.	GS-04 GS-05	987-65-4321

Lotta C. Curity  
 CPT, IN  
 ATASO

**Figure C-4. Combination add, delete, and correction format for bond paper facsimile or cc:mail submission**

Account number: 19005Z  
 Account name: Mesotron Recruiting BN  
 TASO: CPT Artiste N. Lister  
 Effective date: Immediately

Request the following corrections to the ARC3S data base.

USER ID	NAME	GRADE	SSN
5ZSJ89	SMITH, JANE L.	SFC	123-45-6789
	SMITHE, JANE L.		
5ZDJ21	DOE, JOHN K.	GS-04 GS-05	987-65-4321

Lotta C. Curity  
 CPT, IN  
 ATASO

**Figure C-5. Correction format for bond paper facsimile or cc:mail submission**

## Appendix D Automated Data Processing Equipment

### D-1. Purpose

The purpose of this appendix is to identify duties and responsibilities of the TASO that are specific for the operational security of USAREC's ADPE and/or PC.

### D-2. Scope

Each activity or organization will appoint a TASO and ATASO for each PC or contiguous group of PC not under the direct control of an ISSO. Written appointments for TASO and ATASO will be prepared (sample at fig 1) and forwarded to HQ USAREC (RCIM-CE-OP).

### D-3. PC duties of TASO

AR 380-19, paragraph 1-6d(5), USAREC Reg 25-1, and this pamphlet identify duties of the TASO.

NOTE: Wherever reference is made to TASO the same duties and responsibilities apply to the ATASO.

### D-4. General

a. Select a location for the computer and related equipment, when possible, that is free of devices that may cause damage (i.e., water lines, steam radiators, electrical transformers, etc.).

b. Do not eat, smoke, or drink in the immediate vicinity of the computer system.

c. Area fire extinguishers will be checked monthly. If they are found to be nonoperative, steps will be taken to replace them at once.

d. Diskettes are fragile items and misuse or mishandling can damage them. The following procedures should be used when handling diskettes:

(1) Do not place diskettes on terminals, in books, or under equipment.

(2) Do not touch exposed areas or try to wipe diskettes clean.

(3) Keep diskettes out of direct sunlight and away from extreme heat.

(4) Do not place diskettes near any magnetic source such as telephones, radios, tape recorders, speakers, and microwave ovens.

(5) Do not bend diskettes or place rubber bands or paper clips on them.

(6) Do not write directly on diskettes with a ball point pen, pencil, or other hard writing instruments. Use a felt tip pen or write on the label before affixing to a diskette.

(7) Store diskettes vertically in their jackets in either diskette storage trays or boxes to avoid pressure to the sides.

(8) All diskettes will be marked with identification information. Identification information should be at a minimum: User name, organization, type of files on diskette (dBase, MS Word documents, etc.) and, when required, FOUO.

e. Only Government personnel who have a favorable personnel background investigation are authorized to use systems that network. Permission must be granted by the Deputy Chief

of Staff for Operations Security Manager or the ISSO before any other personnel can operate networking systems. All operators of these systems must receive an ISS briefing prior to operating any of the systems.

f. All equipment must be marked with applicable classification it is authorized to process. NOTE: USAREC AIS is accredited to process unclassified sensitive level material only (Privacy Act and FOUO).

g. Copyrighted software may be copied only as explicitly set forth in its contract or licensing agreement. Copyright laws prohibit using the operating disks for any purpose other than installation on the system for which it was purchased. The operating disks for the system will be used only on this system and no other system.

h. Virus protection software has been loaded on all systems. It will not be tampered with and must remain operational on all systems. Any diskette received from outside the organization or by someone within this organization which received it from an outside source, will be checked at the information center for contamination. This check will be accomplished prior to introduction of diskette on any Government system.

i. The USAREC banner must be loaded on all systems. It will not be tampered with and must remain operational to display during boot-up.

j. Any real or suspected infractions of security will be immediately reported to the TASO, ISSO, or the section supervisor.

### D-5. PC responsibilities of TASO

a. Identify PC users based on need-to-know, job relation, and mission requirements.

b. Ensure that USAREC Label 19 is attached to the top of the keyboard.

c. Install antivirus protection, as made available, on every PC and ensure that it remains installed.

d. Ensure that the default autoexec.bat "Anti-virus boot-up installation" is maintained on every PC.

e. Ensure that the USAREC banner (see fig D-1) is maintained to display on every PC during boot-up.

f. Report hardware terminal problems to the local ISSO or IMO.

g. Report missing equipment to the local ISSO or IMO.

h. Report software problems to the local ISSO or IMO.

i. Conduct periodic reviews to prevent illegal and/or unauthorized software.

j. Report possible or actual viruses and/or terminal security violations to the ISSO.

k. Complete and submit a virus report to the ISSM.

l. Inform all PC users of their duties (see para D-6).

### D-6. Responsibilities of PC users

a. New ADPE users are required to apply to the TASO for an initial security briefing. As part of the briefing, new users will be required to read

and sign a company security SOP.

b. Adhere to the security requirements for PC.

c. Handle all information processed on the PC containing personal information as highly sensitive data and comply with the provisions of the Privacy Act of 1974, AR 340-21, and as follows:

(1) Personal information is guarded in the same way as FOUO.

(2) Data transferred to diskettes governed by the Privacy Act and/or FOUO disk will have diskettes marked FOUO and diskettes will be treated in the same manner as "hard copy" FOUO material.

(3) Privacy Act or FOUO "hard copy" output will be marked and handled accordingly.

(4) Privacy Act or FOUO data should only be visible on the monitor when an authorized PC user is present and using equipment. Prior to departing, each user must properly save and close out of a program to prevent inadvertently exposing sensitive data.

d. Ensure that the autoexec.bat is not altered to prevent antivirus software installation during boot-up.

e. Ensure that the USAREC banner is displayed during boot-up.

f. Secure the system, all diskettes associated with the system, and contact the TASO immediately upon detecting a possible or actual virus and/or terminal security violations.

g. Suspected or actual terminal security violations will be reported to the appropriate TASO, who in turn will contact the ISSO.

h. Users will not smoke, eat, or drink at a terminal or workstation.

i. Use of passwords with ADPE.

(1) Authorized users will not allow another individual to use their unique user ID and password.

(2) Personal passwords are not to be given to unauthorized users or left out in plain view.

(3) Attempt to access or actual access by posing as an authorized user (with their user ID) is termed masquerading or mimicking and is a security violation.

(4) Old passwords and sensitive information (FOUO) should be destroyed by tearing, shredding, or mutilating to render personal data unrecognizable and beyond reconstruction.

(5) Personal passwords should be changed every 90 days or whenever the user believes their password may have been compromised.

j. Security violations (unauthorized users, passwords not stored as FOUO, etc.) and any loss or theft of automated data processing property must be reported to the TASO.

### D-7. Assistance

a. ISS assistance.

(1) Assistance in identifying AIS security requirements is available from HQ USAREC (RCIM-CE-OP). The appropriate ISSO should request assistance directly from HQ USAREC (RCIM-CE-OP) at 1-800-223-3735, extension 6-0027.

(2) The TASO and/or ATASO should consult

their ISSO for AIS security assistance prior to contacting HQ USAREC (RCIM-CE-OP).

b. General assistance. Users experiencing a problem, either hardware or software, should

contact their TASO or ATASO. Problems which cannot be corrected by the TASO or ATASO should be referred to the USAREC ADP Hot Line at DSN 536-1077 or USAREC Toll Free Number

1-800-223-3735, ext 6-1077. Problems should not be referred to the hot line without prior notification of the TASO or ATASO.

THIS IS A DEPARTMENT OF DEFENSE (DOD) INTEREST COMPUTER SYSTEM (ICS). USE OF THIS OR ANY DOD ICS CONSTITUTES A CONSENT TO MONITORING AT ALL TIMES.

\* \* \* \* \*

All DOD ICS's and related equipment are intended for the communication, transmission, processing, and storage of OFFICIAL U.S. Government or other authorized information ONLY. All DOD ICS's are subject to monitoring at all times to ensure proper functioning of equipment and systems including security systems, to prevent unauthorized use and violations of statutes and security regulations, to deter criminal activity, and for other similar purposes. Any user of a DOD ICS should be aware that ALL information placed in the system is subject to monitoring and is not subject to any expectation of privacy.

If monitoring of this or any other DOD ICS reveals possible evidence of violation of criminal statutes, this and any other related information, including user identification, may be provided to law enforcement officials. Employees violating security regulations or making unauthorized use of DOD ICS's are subject to appropriate disciplinary action.

DOD ICS users are to comply with software copyright laws and licensing agreements.

\* \* \* \* \*

THIS EQUIPMENT WILL NOT BE USED TO PROCESS CLASSIFIED MATERIAL.

\* \* \* \* \*

Figure D-1. PC warning banner

## Appendix E

### Information Systems Security Briefing for Users, Supervisors, and Managers of Automated Information Systems

1. Introduction. In December 1987, Congress passed the "Computer Security Act of 1987." In January 1988, that Act became Public Law 100-235. The Law set forth a statutory requirement that all users, supervisors, and managers of automated information systems (AIS) receive initial and annual training in automation security. This same requirement is also regulatory under AR 380-19, paragraph 2-6. The following briefing fulfills the training requirements of both Public Law 100-235 and AR 380-19.

2. Purpose of Information Systems Security. Thousands of AIS operate in the U.S. Government processing classified and unclassified sensitive information. These systems are vulnerable to computer hackers, hostile intelligence agents, thieves, and individuals with malicious intent. The rapid increase in AIS over the last few years has made security a major issue concerning the safeguarding of systems and most importantly, the data they process. The Information Systems Security Program defines various threats to our AIS and applies countermeasures. The program is designed to protect against the following types of threats:

- a. Espionage.
- b. Compromise or unauthorized manipulation of classified and sensitive unclassified information.
- c. Unintentional loss or malicious destruction of data files.
- d. Malicious or unintentional damage to or destruction of AIS hardware and software.
- e. Theft of hardware and software.
- f. Unauthorized use of software that may contain malicious programs (e.g., computer viruses, logic bombs, etc.).
- g. Unauthorized personal use of AIS.
- h. Natural disasters which would destroy AIS resources, data bases, or otherwise interrupt AIS services.
- i. An authorized AIS user who is ignorant of security policies and procedures.

#### 3. Personal Responsibility.

a. If you are a manager, supervisor, or user of AIS operations, you are required under the law to apply prescribed security policies and procedures. Failure to do so may subject you to disciplinary action and penalties under the law. Information systems security policies and procedures are found in Army regulations and USAREC publications, unit standing operating procedures, and in this document.

b. Before you begin operating an AIS, be sure you understand and comply with the security requirements of the system. Ask your information systems security officer (ISSO) or your terminal area security officer (TASO) if you have any questions.

c. You are responsible for compliance with the following automation security policies and procedures which are divided into four areas: Procedural security, data security, physical security, and communication security. These policies and procedures are not all inclusive; however, they constitute the minimum "do's and don'ts" of system operation.

4. Procedural Security. Procedural security dictates how you operate and maintain your system. Users, supervisors,

and managers will:

- a. Obtain an automation security briefing from their ISSO or TASO before using AIS equipment (this briefing fulfills the requirement).
- b. Ensure that AIS equipment is maintained with care (for example, used properly, kept clean). The processing environment must also be kept as clean as possible. Smoking is not allowed in areas where AIS operate.
- c. Operate AIS equipment according to operation reference manuals and posted security instructions.
- d. Ensure that the ISSO has approved and accredited software packages before they are used. Personal copies of software are prohibited in the workplace for use on Government-owned equipment.
- e. Ensure that no additional equipment is attached to an AIS without the knowledge and permission of the ISSO. Attaching additional equipment will require additional accreditation.
- f. Honor software copyright restrictions. No unauthorized copies of copyright software may be made for office or personal use. Copyright software may not be borrowed or removed from the workplace.
- g. Do not load copyright software onto other AIS unless authorized in vendor agreements.
- h. Protect against disaster. Always have backup copies of application programs and data files ready to go. Update backup copies of data files regularly.
- i. Safeguard assigned user passwords. Do not reveal passwords to anyone, and do not store them in plain text on an AIS.
- j. Report compromised passwords to the ISSO or TASO.
- k. Protect equipment. Keep food, drink, and electrical appliances away from an AIS.
- l. Protect any unattended terminal. Always log-out of an AIS terminal or turn off a computer before leaving it unattended.
- m. Protect against viruses. Never introduce diskettes or media obtained outside the work arena onto a Government system before having it checked for a virus. Talk to your ISSO or TASO on your location's procedures. Obtain software only from recognized Government agencies when possible, and even check those medias for virus contamination prior to introducing it to a Government system.
- n. Report immediately any suspected computer misuse or abuse to the ISSO or TASO.

5. Data Security. Always protect classified and unclassified sensitive information. Classified data products must be safeguarded (processed and stored) under the provisions of AR 380-5. For Official Use Only (FOUO) sensitive and mission-critical information and Privacy Act information require protection from disclosure, alteration, and loss. Users, supervisors, and managers will:

- a. Protect data systems:
  - (1) Establish and periodically review access privileges for each data system.
  - (2) Inspect data files for tampering. If you suspect someone has tampered with your files or the data in them, report it immediately to your ISSO or TASO.

(3) Do not attempt to access any data on any AIS or computer network unless you have been specifically authorized such access.

(4) Do not process data that exceeds the accreditation sensitivity level of the AIS. If you are unsure, ask your ISSO or TASO. The USAREC host systems and personal computers are not accredited to process classified material.

(5) Do not allow anyone to access a data system unless the person has a job or mission requirement or need-to-know that is verified by the ISSO or TASO.

b. Protect data media.

(1) Secure removable media and equipment that contains fixed media.

(2) Secure backup diskettes and/or tapes.

(3) Label sensitive diskettes with the classification of the data (FOUO and Privacy Act) stored on them.

(4) Secure diskettes with sensitive data to prevent easy access to data.

(5) Handle diskettes carefully to avoid damage. Avoid touching exposed areas, magnets, and magnetic fields (i.e., telephones, electrical wiring, power strips, etc.).

(6) Do not write on a diskette with pencil or pen. Any writing on a label after it is attached to a diskette should be done with a soft felt pen.

(7) Avoid using a personal computer's fixed "hard" disks for sensitive data storage except when large data bases make this impractical.

c. Protect data output.

(1) Mark sensitive data output products at the top and bottom of the page with the proper classification (FOUO, Privacy Act) or use DA Label 87 (For Official Use Only Cover Sheet) as appropriate.

(2) Dispose of waste containing sensitive information properly (for example, FOUO approved recycling, burning, or shredding).

(3) Secure sensitive AIS data products from open sight or easy access.

6. Communications Security. The following policies and procedures apply to AIS that are networked, including systems with dial-up modem capability. Users, supervisors, and managers will:

a. Ensure that information transmitted by modem (telecommunications) is not classified or sensitive and the transmission of the information type has been approved by the ISSO or TASO. If in doubt as to what is sensitive, consult with your security personnel.

b. Turn off an AIS or disconnect it from the network when not in use. An active AIS connected to a network or to another AIS can be accessed and files, applications, and even the operating system can possibly be changed without your knowledge.

c. Use electronic mail (E-mail) systems FOUO. E-mail will not be used for transmission and receipt of classified communications. Unclassified sensitive (FOUO and Privacy Act data) should not be sent to an open system where someone other than the addressee could receive it. Be extremely careful what and how you send over E-mail.

7. Physical Security. Physical security limits access to your processing environment and provides security for your AIS. AIS users and their supervisors must:

a. Protect data processing areas. Recognize, politely challenge, and assist people who do not belong in your area.

b. Limit access to AIS. Know those who are authorized to use, service, and repair your AIS. Use system lock-down or power switch locking devices when available.

c. During nonduty hours and when offices are left unattended, lock office doors and rooms which house AIS equipment.

d. Restrict access to areas where classified information is being processed.

e. Ensure that AIS hardware and software are hand-receipted by serial numbers to users, sections, or office chiefs. Hardware and software must have an accountability chain back to the property book officer.

f. Challenge persons carrying AIS components out of an office or building. They may be in the process of stealing it.

g. Do not allow any AIS hardware to be moved from its accredited location without the knowledge and approval of the ISSO. This includes turning in equipment for maintenance.

h. Do not allow storage media on which classified and/or sensitive data or applications have resided to leave controlled channels until they have been declassified.

8. Personal Liability for Fraud and Criminal Activity in Connection With Computers. (Ref Title 18, U.S. Code.) AIS users, supervisors, and managers must be aware of the following:

a. Federal law provides for punishment of up to \$100,000 and 1 year in jail for the first offense of anyone who:

(1) Knowingly accesses a computer without authorization, or exceeds authorized access, and obtains information which requires protection against unauthorized disclosures.

NOTE: The offense is for the access and not necessarily any disclosure.

(2) Intentionally, without authorization accesses a Government computer and, in so doing, affects the use of the Government's operation of the computer.

(3) Intentionally accesses a Government computer without authorization, and alters, damages, or destroys information or prevents authorized use of the computer.

(4) Accesses a Government computer without authorization or exceeds authorized access and obtains anything of value.

b. The above prohibitions and punishments apply to mere attempts - even if unsuccessful - to commit the listed crimes. Multiple accesses, or multiple attempts constitute multiple offenses for the purposes of determining punishment.

9. Acknowledgment. Users, supervisors, and managers will acknowledge by signature that they have read and understood the above instructions. Any questions regarding these instructions must be answered by the ISSO or TASO (briefer) prior to signature. Persons who refuse to acknowledge the briefing will not be allowed to operate an



## Appendix F Software

### F-1. Purpose

The purpose of this appendix is to identify duties and responsibilities of the TASO that are specific for the operational security of USAREC's software.

### F-2. Scope

Each activity or organization will appoint a TASO and ATASO for each PC or contiguous group of PC not under the direct control of an ISSO. Written appointments for TASO and ATASO will be prepared (sample at fig 1) and forwarded to HQ USAREC (RCIM-CE-OP) or submitted via facsimile (502) 626-0912.

### F-3. Software duties of TASO

AR 380-19, paragraph 1-6d(5), USAREC Reg 25-1, and this pamphlet identify duties of the TASO.

NOTE: Wherever reference is made to TASO the same duties and responsibilities apply to the ATASO.

### F-4. General

a. Unless specific written permission has been granted by the software licensor, no individual has the right to copy, reproduce, merge, modify, or transfer all or any portion of the software. The copyright law permits making a single backup copy, the licensing agreement accompanying the software will state any other rights granted the licensee. When manufacturers copy-protect their software, they will normally provide a backup or archival copy of software to the purchaser.

b. All personnel must abide by the provisions of the software license agreement that accompanies the software. Under no circumstances are employees permitted to make copies for their personal use.

c. The licensor software registration materials will be processed promptly. All software will be registered to the using activity's name (i.e., Commander, Fourth Recruiting Brigade or Director, Software Control Directorate, etc.) and address and not the individual user.

d. When commercial software packages are superseded, upgraded, or reach an automatic expiration date the licensee registered with the software vendor must ensure previous software versions are disposed of properly. Each IMO will ensure that disposition instructions are issued when software packages are distributed. Since each type of software has unique disposition requirements, adherence to these instructions will ensure that neither the user nor the Government becomes liable for infringement of commercial software copyright laws and/or licensing agreements.

e. Software declared obsolete or excess will be returned to the IMO for further disposition.

f. All software will be cleared from PC prior to turn-in for redistribution or transfer, unless directed otherwise by the IMO.

g. Only software that has been specifically developed, approved for use, and/or purchased

or leased by an authorized Government representative will be used within USAREC. Government purchased "off-the-shelf," privately purchased, public domain, shareware, freeware, or software obtained from any source will not be used unless prior approval by the Director of Information Management has been obtained. Employees will not use Government-owned equipment to copy and/or download software, of any type from the internet, bulletin boards, or other sources for their personal use.

h. Prior approval must be obtained from the Director of Information Management before any non-Government licensed software (including public domain and shareware) may be used on Government-owned equipment. The TASO will coordinate a request for authorization with the immediate supervisor and the IMO. The IMO will then forward the request provided the use of software is not in conflict with nor corrupts Government-owned resources. The request must be submitted to and approved by the Director of Information Management. If the approval is granted, the IMO will provide the TASO with written authorization to use the software package and satisfy audit requirements. For any non-Government licensed software to be considered for approval, by the Director of Information Management, it must comply with the following:

(1) Software is not in violation of license and/or copyright laws or constraints.

(2) Software is used only for Government work.

(3) Software has been tested for viruses.

(4) Product is clearly marked "Non-Government Software."

(5) Software is not used to create "mission critical" application.

i. For auditing purposes, all software installed on a system (PC, server, etc.) must be documented for legal use. The original media (i.e., floppy diskettes or compact disks) used for installation is the preferred software documentation. Systems with preinstalled software that did not include an original media must have procurement, shipping, receipt, or other documents to substantiate the software's legality.

### F-5. Software responsibilities of TASO

a. Receive, sign for, ensure proper installation, and maintain close and continuous management controls for Government licensed software packages.

b. Register Government licensed software and/or ensure it is properly registered with vendor.

c. Issue user required instructions, manuals, or relevant materials.

d. Receive and ensure proper installation of vendor update packages and distribute any associated newsletters and/or publications.

e. Ensure obsolete, superseded, or excess software is deleted from the system and follow procedures for its handling, disposing, and/or turn-in.

f. Develop local procedures for software inventory and management. Procedures should include: Name of software package (i.e., Enable, WordPerfect, Dbase IV, etc.), version of the

package (i.e., 1.0, 3.2, etc.), number of diskettes per package (i.e., six Dbase IV, eight Harvard Graphics, etc.), applicable serial number of each software package, and identity of the system on which it is installed.

g. Monitor and control all commercial software and documentation for the area of responsibility.

h. Conduct annual inventory of all Government-licensed commercial software and documentation.

i. Direct the removal of all unauthorized or undocumented software found during routine checks or inventory.

j. Report lost, stolen, or damaged commercial software (original and/or authorized archival copy) and/or software documentation. The report must specify, at a minimum, the prompt reporting of the incident and all identifying information (e.g., serial numbers to the IMO or ISSO).

k. Inventory and verify all manuals and/or documents, which were issued, are accountable prior an employee's departure.

l. Follow basis of issue and/or IMO instructions for disposition of commercial software and documentation when information system resources are transferred between user or elements.

m. Ensure all Government-owned and non-Government-owned software is tested for computer viruses prior to installation.

n. Ensure authorization is obtained prior to any non-Government licensed software being used on Government-owned equipment.

### F-6. Software responsibilities of users

a. Abide by the provisions of commercial software license agreements and/or copyright laws or constraints relative to commercial software.

b. Practice procedures necessary to ensure neither the user nor the Government becomes liable for infringement of commercial software copyright laws.

c. Follow guidance contained in this pamphlet (specifically para F-4).

### F-7. Assistance

a. ISS assistance.

(1) Assistance in identifying AIS security requirements is available from HQ USAREC (RCIM-CE-OP). The appropriate ISSO should request assistance directly from HQ USAREC (RCIM-CE-OP) at 1-800-223-3735, extension 6-0027.

(2) The TASO and/or ATASO should consult their ISSO for AIS security assistance prior to contacting HQ USAREC (RCIM-CE-OP).

b. General assistance. Hardware and software assistance is available from the Information Management Help Desk at 1-800-223-3735, extension 6-1077. Individual AIS users requiring assistance should consult with their TASO and/or ATASO for solving problems or assistance prior to contacting the ISSO, ISSM, or Help Desk.

## Appendix G Viruses

### G-1. Purpose

The purpose of this appendix is to identify duties and responsibilities of the TASO and AIS users that are specific for virus prevention, detection, eradication, and/or reporting.

### G-2. Scope

Each activity or organization will appoint a TASO and ATASO for each terminal or contiguous group of terminals not under the direct control of an ISSO. Written appointments for TASO and ATASO will be prepared (sample at fig 1) and forwarded to HQ USAREC (RCIM-CE-OP).

### G-3. Duties of TASO

AR 380-19, paragraph 1-6d(5), USAREC Reg 25-1, and this pamphlet identify duties of the TASO.

NOTE: Wherever reference is made to TASO the same duties and responsibilities apply to the ATASO.

### G-4. General

a. Virus protection software will be loaded on all systems. It will not be tampered with and must remain operational on all systems.

b. Know and be comfortable with the source of your software acquisitions. A PC virus must be physically introduced into a system via diskette or other physical link such as a modem or hard connection to a LAN or other server. Only use software that has come through appropriate channels and has been scanned.

c. Viruses are generally introduced through "friendly" hands that have access and opportunity. Most viruses are introduced by the PC's regular operator, though someone who "borrows" a PC to look at or use a diskette may infect the system.

d. Do not use illegitimate copies of software. This is especially true with bulletin boards, shareware, freeware, or unsolicited demo and game software. Virus authors generally employ subtle methods to get you to introduce the virus into the system. More often they can be traced to an inexpensive or free game, utility, or demo diskette.

e. Treat all diskettes and software as suspect. No diskette source can be certified as 100 percent virus safe, viruses have been reported in new boxes of blank preformatted and shrink wrapped program diskettes.

f. Never boot your system from a diskette you're unsure of and always keep a "write-protect tab" on your system boot diskette.

g. With a hard disk system, get in the habit of always making sure that the door to your "A" drive is open whenever you turn the system on or whenever you reboot. This will prevent an accidental boot attempt from a diskette that may be in the "A" drive.

h. Never execute programs of unknown origin.

i. Make sure that the service companies and

repair personnel are aware of the virus situation and that they practice care in the treatment of the diskettes they use.

j. Backup your data files on a regular schedule, using multiple sets of backup disks.

k. Treat strange or unusual system operation and/or messages as a potential virus infection.

l. Know that after a virus infection has occurred there is a high probability of a reinfection within 30 days.

### G-5. Virus responsibilities of TASO

a. Ensure that the system's autoexec.bat file "loads" the command standard antivirus software during boot-up.

b. Conduct periodic spot checks to ensure the autoexec.bat file is not altered to prevent the command standard antivirus software from loading during system boot-up.

c. Install the latest version command standard antivirus software, as made available, on every PC and conduct periodic spot checks to ensure that it remains installed.

d. Report possible or actual viruses to the ISSO or IMO and, if necessary, request assistance to detect and eradicate.

e. Isolate the system and all diskettes that have been in contact with the system. This includes an immediate disconnection from the LAN.

f. Run the command standard scan and clean virus program on the infected system and all diskettes that have been in contact with the system.

g. Run the command standard scan and clean virus on all other systems and diskettes that are in the vicinity of the infected system.

h. Run the command standard scan and clean virus program on all other systems and diskettes that may have conducted any type of data transfer with the infected system.

i. Try to determine the infection's originating source by interviewing system users.

j. Notify the ISSO or IMO when the virus is eradicated and how extensive its infection.

k. Complete and submit a virus report to the ISSM (see fig G-1 for sample). The virus report will include: Date discovered, individual who discovered virus, first indication of infection, virus identified, location, extent of infection, actions taken to detect and eradicate, source or probable source, preventative measures, and any other actions taken.

l. Closely monitor the infected area during the next 30 days then spot check during an additional 60 days for potential reinfections.

m. Inform all PC users of their duties (see para G-6).

### G-6. Responsibilities of PC users

a. Ensure that the system's autoexec.bat file loads the command standard antivirus software during boot-up.

b. Notify the TASO should the command standard antivirus software fail to load during system boot-up.

c. Report suspected or actual viruses and/or

terminal security violations to the TASO.

d. When suspected or actual virus is discovered, turn the system off and attach a note to its screen that states, "Suspected virus, do not use this system."

e. Document the events that indicated a suspected or verified that the system was infected.

f. Secure all diskettes that have been in contact with the system.

g. Ensure that all diskettes that have been in contact with the system are provided to the TASO for scanning.

h. Provide the TASO information as to other systems and diskettes that may have been in contact with the infected system.

i. Provide the TASO any information that may aid in determining the virus' origin.

j. After a virus has been detected do not use any diskettes not marked as scanned until the TASO has verified the virus has been eradicated.

k. After a virus has been detected do not use any diskettes found at a later date that were used on the system but not scanned and cleaned prior to the TASO scanning and certifying they are virus free.

### G-7. Procedures to detect and eradicate

The procedures listed here are intended for a general guide. Procedures to detect and eradicate may vary dependent upon the type of an infection. Anyone experiencing an infection that requires additional information and/or guidance should follow the procedures for assistance in paragraph G-8.

a. Individual suspects or finds an actual virus on a system.

b. Individual notifies TASO that suspected or actual viruses have been discovered.

c. If TASO is not in the area and immediately available the user turns the system off and attaches a note to its screen that states, "Suspected virus, do not use this system."

d. Individual documents events that indicated the system was infected.

e. Individual secures all diskettes that have been in contact with the system.

f. TASO isolates and checks system to confirm or refute actual virus infection.

g. TASO reports viruses to the ISSO or IMO and, if necessary, requests assistance to detect and eradicate.

h. TASO scans and/or cleans the system.

i. Individual provides TASO all diskettes that have been in contact with the system for scanning and/or cleaning.

j. TASO uses visual indicator (i.e., felt marker large blue C and/or red X) to indicate diskettes that have been scanned and cleaned or are infected.

k. TASO certifies that system and diskettes, marked accordingly, are clean and informs the AIS user that they are not to use any diskettes not marked as clean until the TASO certifies the virus is eradicated.

l. Individual informs TASO as to other systems and/or diskettes that may have been in contact with the infected system.

m. TASO repeats steps in f through l above until infection is eradicated.

n. TASO notifies AIS users when the virus is eradicated at the activity.

o. TASO interviews users to determine infection's originating source.

NOTE: TASO should interview and not interrogate. It is more important to discover from where and how the infection occurred in order to eliminate it and prevent future occurrences than to attempt to affix blame.

p. TASO notifies the ISSO or IMO when the virus is eradicated and how extensive its infection.

q. TASO completes and submits a virus report to the ISSM.

r. TASO monitors the infected area during the next 30 days and spot checks during an additional 30 days for potential reinfections.

#### **G-8. Assistance**

a. ISS assistance.

(1) Assistance in identifying AIS security requirements is available from HQ USAREC (RCIM-CE-OP). The appropriate ISSO should request assistance directly from HQ USAREC (RCIM-CE-OP) at 1-800-223-3735, extension 6-0027.

(2) The TASO and/or ATASO should consult their ISSO for AIS security assistance prior to contacting HQ USAREC (RCIM-CE-OP).

b. General assistance. Hardware and software assistance is available from the Information Management Help Desk at 1-800-223-3735, extension 6-1077. Individual AIS users requiring assistance should consult with their TASO and/or ATASO for solving problems or assistance prior to contacting the ISSO, ISSM, or Help Desk.

Appropriate Letterhead

OFFICE SYMBOL

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Virus Report

1. Date Discovered: 15 June 1995 (self-explanatory).
2. Discovered By: Ben N. Fektid (self-explanatory).
3. First indication of Virus (*what caused individual to suspect presence of virus*):
  - a. System locked when attempting to access data diskette and displayed message "stoned-b virus detected on drive a."
  - b. System displayed message "Your PC has been stoned, legalize marijuana."
  - c. System was operating noticeably slower.
4. Virus identified: Stoned-B (self-explanatory).
5. Initial Discovery Location: Influenza Recruiting Battalion, Admin Computer (self-explanatory).
6. Extent of Infection: Influenza Recruiting Battalion, Admin Computer (if more than one system infected use a, b, etc., as below).
  - a. Influenza Recruiting Battalion, Admin Computer.
  - b. Influenza Recruiting Battalion, Operations Computer.
  - c. Influenza Recruiting Battalion, Supply Computer.
7. Actions taken to detect and eradicate (*detail methods to detect and eradicate*): Used McAfee Version 221 to scan and clean Admin PC and all diskettes, operator reported a data diskette was exchanged several times between Admin and Operations. Repeated scan and clean procedures with Operations PC, operator reported receiving a data diskette from Supply. Repeated scan and clean procedures with Supply PC. Conducted scan on PC in vicinity of Admin, Operations, and Supply and did not detect any other viruses.
8. Source/Probable Source (*based on user interview attempt to determine source*): One-way exchange with data diskette from Supply PC indicates virus most likely origin point. Contract repairman had recently performed maintenance and used diagnostics software on Supply PC. Repairman or other party had altered Supply PC autoexec.bat file to prevent virus protection from loading during boot. The Operations PC autoexec.bat file had also been altered to prevent virus protection from loading during boot. Unable to determine who altered batch files.

**Figure G-1. Sample virus report**

OFFICE SYMBOL  
SUBJECT: Virus Report

9. Preventative Measures (*measures to educate users and/or prevent reoccurrence*): Had AIS users read USAREC Pam 380-5, appendix G. Informed AIS users that they were required to inform the TASO if the virus protection failed to load during boot. Informed AIS users to notify the TASO immediately whenever outside diskettes were used on Government PC.

10. Other Actions (*any other applicable preventative actions*): Notified contracted repairman that diagnostics diskettes were possibly infected.

TASO Signature Block

DISTRIBUTION:  
RCIM, ISSM  
ISSO  
TASO File

**Figure G-1. Sample virus report (Continued)**

## **Glossary**

### **ADPE**

automated data processing equipment

### **AIS**

automated information system

### **AISSP**

U.S. Army Information Systems Security Program

### **ARADS**

Army Recruiting and Accession Data System

### **ARC3S**

Army Recruiting Command Central Computer System

### **ATASO**

alternate terminal area security officer

### **CIMS**

Command Integrated Management System

### **FOUO**

For Official Use Only

### **HQ USAREC**

Headquarters, United States Army Recruiting Command

### **ID**

identification

### **IMO**

information management officer

### **ISS**

information systems security

### **ISSM**

information systems security manager

### **ISSO**

information systems security officer

### **ISSPM**

information systems security program manager

### **LAN**

local area network

### **PC**

personal computer

### **Rctg Bde**

recruiting brigade

### **Rctg Bn**

recruiting battalion

### **RSID**

recruiting station identification

### **SOP**

standing operating procedures

### **SSN**

social security number

### **TASO**

terminal area security officer

### **USAISC**

United States Army Information Systems Command

### **USAREC**

United States Army Recruiting Command

**INFORMATION SYSTEMS SECURITY CHECKLIST**

(For use of this form see USAREC Pam 380-5)

YES	NO	N/A

**1. TASSO AND ATASSO:**

- a. Has a terminal area security officer (TASSO) and alternate terminal area security officer (ATASSO) been appointed for each interconnected computer and terminal, or group of contiguous terminals?
- b. Is the TASSO and ATASSO properly appointed in writing? If so, attach letter of appointment to this document. If not, obtain letter of appointment and attach to this document.
- c. Does the TASSO and ATASSO have a copy of AR 380-19?
- d. Does the TASSO and ATASSO ensure that instructions specifying security requirements and operating procedures are available for each terminal area he or she is responsible for?
- e. Has the TASSO and ATASSO ensured that each terminal user's identification (ID), need-to-know, level of clearance, and access authorization is established commensurate with the data available from that terminal?
- f. Does the TASSO and ATASSO manage the control and dissemination of user and file ID numbers and default passwords?
- g. Is the TASSO and ATASSO aware of who accesses the terminal(s) and what outputs are printed from the terminals?
- h. Does the TASSO and ATASSO mark, handle, process, and store Privacy Act and For Official Use Only (FOUO) data, printouts, and diskettes accordingly?
- i. Has the TASSO and ATASSO implemented controls to prevent entry of unauthorized transactions of data (e.g., classified data over unsecured data transmission lines)?
- j. Does the TASSO and ATASSO check and ensure that remote terminals are available only to authorized individuals?
- k. Does the TASSO and ATASSO conduct periodic training in regards to existing regulations and procedures governing the proper usage of the terminal and sign-on and sign-off procedures?
- l. Does the TASSO and ATASSO check and ensure that terminal boards and other communications equipment associated with the teleprocessing computer system are located in locked rooms where access has been strictly controlled?
- m. Where possible, is the TASSO's and ATASSO's terminal located to assure privacy and prevent viewing of entry features by unauthorized individuals?
- n. Has the TASSO and ATASSO changed the default to a personal password?
- o. Is the TASSO's and ATASSO's personal password known only by the user?
- p. Does the TASSO and ATASSO enforce local compliance with security operating procedures for that terminal?
- q. Is the TASSO and ATASSO performing all possible actions to assist the host system information systems security officer (ISSO) in ensuring that overall system security is being affected?

**2. PHYSICAL AND ENVIRONMENTAL:**

- a. Are positive physical access controls established to prevent unauthorized entry into the area where computer equipment is located?
- b. Are the buildings or facilities selected to house computer equipment sufficient structural integrity so as to provide, or capable of being made, to provide effective physical security at a reasonable cost?
- c. Do the physical characteristics of the location selected to house the automated system support the establishment of an effective physical security system at the facility?
- d. Is the computer area secured upon completion of the duty day or at any time the facility is unmanned?

- e. Is strict accountability maintained over keys, combinations, or identification numbers which permit access to the facility?
- f. Is there an organization or activity representative present during janitorial cleaning operations?
- g. Are areas containing remote terminals secured during and after hours consistent with the level of information accessed by the terminal?
- h. Are positive administrative safeguards being implemented to ensure that only authorized individuals are permitted to utilize remote terminal equipment capable of accessing the computer systems?
- i. Has adequate fire protection for mission-essential automated systems been achieved through a combination of minimizing the exposure to fire damage by assuring prompt detection and by providing adequate means to extinguish the fire?
- j. Have conflicts between security and fire safety requirements been brought to the attention of the commander?
- k. Within the facility, have good housekeeping and operating procedures been prerequisites to maintaining a noncombustible environment?
- l. Have the use of tobacco products, eating, and drinking been strictly prohibited in the areas where automated data processing equipment is being used?
- m. Has a minimum degree of fire protection, primarily being handheld extinguishing equipment, been implemented with additional protection provided by an area extinguishing system or systems, as appropriate?
- n. Is fire extinguishing equipment immediately available for use in controlling fires in a computer equipment area?
- o. Are a sufficient number of carbon dioxide (CO2) extinguishers available for use in case of nonelectrical fires and installed in accordance with NFPA Code 10?
- p. Are water type fire extinguishers also available for use on nonelectrical fires?
- q. Are handheld extinguishers marked to indicate the type of fire for which they are intended?
- r. Have commanders ensured that orientation and training classes are held to enable personnel who work around computer equipment to become familiar with facility fire equipment (emergency) and procedures?
- s. Are cost effective security measures implemented to ensure that sensitive information is properly protected at all times?
- t. Is the environmental protection consistent with the equipment manufacturer's recommendation?
- u. Is fire protection achieved by the installation of local smoke alarms and portable extinguishing equipment?
- v. Has the commander at each facility assured that adequate procedures have been established to obtain firefighting assistance from the local fire department?
- w. Is office equipment properly safeguarded?
- x. Are expendable supplies properly safeguarded?
- y. Are communication-electronic items provided adequate security?
- z. Are adequate inspections being made to determine the effectiveness of the Information Security Program both within activities and in subordinate elements?
  - aa. Are information and material afforded protection commensurate with the level of classification assigned?
  - ab. Are material and diskettes properly marked with the overall classification (FOUO, Privacy Act)?
  - ac. Are FOUO material and diskettes being properly safeguarded?
  - ad. Are FOUO material and diskettes being properly destroyed?

YES	NO	N/A

YES	NO	N/A

**3. PERSONNEL SECURITY:**

a. Have all automation personnel been provided an appropriate security briefing upon arrival at the organization or activity before beginning their assigned duties?

b. Do security briefings include information on AR 380-19:

- (1) Duties individual is expected to perform?
- (2) Local security environment?
- (3) Computer hardware and software?
- (4) Individual security responsibilities?

c. Has a continuing security education program been established?

d. Where required, are users checked to ensure that they have undergone a satisfactory security background check before issuance of a user ID and password?

e. Are user ID issued on a need-to-know, job relation, and mission requirements basis?

f. Are user ID promptly deleted for users that no longer require access due to change in operational requirements or departure?

**4. COMMUNICATIONS SECURITY AND TERMINAL ACCESS:**

a. Is the responsibility for issuance and control of all system's user ID handled by the TASO or ATASO?

b. After generation, are systems user ID handled and stored at the level of FOUO?

c. At the time of user ID and password issuance, are users briefed on password protection, methods to safeguard, unauthorized use, and to inform the TASO or ATASO of misuse?

d. Are personal passwords changed periodically?

e. Are all cases of actual or suspected compromise of a given password investigated immediately by the TASO or ATASO and reported to the ISSO?

**5. SOFTWARE:**

a. Are there provisions that ensure all software is accounted for?

b. Is software being used within the manufacturer's licensing agreement?

c. Are operators informed of requirements and procedures to protect the integrity of software manufacturer's licensing agreement?

d. Are the master copy diskettes write protected, properly stored, safeguarded, and never used for actual production operations?

e. Is the "latest" version of antiviral software being employed?

**6. PROCEDURAL:**

a. Does the TASO and ATASO maintain a current host system user access roster of all personnel authorized access to the system?

b. Does the system user access roster contain the name, grade, organization, user ID code, and function applicable?

c. Are interval procedures for the following established:

- (1) Fire evacuation?
- (2) Activating fire alarms?
- (3) Fire and police help?

YES	NO	NA

(4) Safety do's and don'ts:

(a) For operating equipment?

(b) Smoking, eating, and drinking areas?

(c) Site cleanliness?

d. Are there policies and procedures for positive control of portable terminals to prevent their theft and misuse?

e. Are personal passwords known by only one user?

f. Are passwords changed periodically?

g. Have procedures been established for the continuing protection of automated data processing files, application and system software, and the system documentation?

h. Is local compliance with security operating procedures for that terminal site being enforced?

i. Are all possible actions to assist the host system ISSO in ensuring overall system security being effected?

**7. RISK MANAGEMENT:**

a. Has a risk management assessment been performed?

b. Is the review of identified risks and determining appropriate countermeasures a function of top level management?

**8. PRIVACY SAFEGUARDS FOR AUTOMATED SYSTEMS:**

a. Does the automated data processing system(s) process or store any Privacy Act information?

b. Are Privacy Act waste products being properly disposed of?

c. Are Privacy Act output products and storage media labeled FOUO - PRIVACY ACT DATA?

**9. REQUIRED DIRECTIVES:**

a. Does the command have the following publications on hand and current:

(1) AR 25-1 (The Army Information Resources Management Program)?

(2) AR 340-21 (The Army Privacy Program)?

(3) AR 380-5 (Department of the Army Information Security Program)?

(4) AR 380-19 (Information Systems Security)?

(5) AR 380-53 (Communications Security Monitoring)?

(6) AR 380-67 (Department of the Army Personnel Security Program)?

(7) AR 710-2 (Inventory Management Supply Policy Below the Wholesale Level)?

(8) DA Pam 710-2-1 (Using Unit Supply System (Manual Procedures))?

b. Does the command have on hand and use:

(1) USAREC Label 19?

(2) USAREC Poster 7?

(3) USAREC Poster 15-R?

(4) DD Form 2056?



**ARADS USER ACCESS REQUEST (Headquarters and Staff Elements)**

(For use of this form see USAREC Pam 380-5)

**Information Required By the Privacy Act of 1974**

**Authority:** 5 USC 522A, Public Law 93-579, AR 340-21, and AR 380-19.

**Principal Purpose:** Used to identify and authorize AIS users and assign user identification (ID) codes required to access USAREC host systems.

**Routine Uses:** To assign individual's user ID code(s) and add user ID for access to USAREC host system(s).

**Disclosure:** Voluntary. Failure to furnish the information requested will result in denial of user ID(s) issuance and access to USAREC host system.

**User ID are issued to individuals based on need-to-know, job relation, and mission requirements.**

**Print or Type User Data**

1. NAME: \_\_\_\_\_ 2. GRADE/RANK: \_\_\_\_\_ 3. SSN: \_\_\_\_\_

4. ORGANIZATION: \_\_\_\_\_ 5. DUTY POSITION: \_\_\_\_\_

6. DUTY TELEPHONE: COMMERCIAL: ( ) \_\_\_\_\_ DSN: \_\_\_\_\_ 7. DATE: \_\_\_\_\_

**HEADQUARTERS AND STAFF ELEMENTS**

**RECRUITING**

**HUMAN RESOURCES**

**ADVERTISING AND SALES**

\_\_\_\_ HQ-RO-ADMIN

\_\_\_\_ HQ-AGR

\_\_\_\_ HQ-BUDGET & ACCOUNTING

\_\_\_\_ HQ-RO-E

\_\_\_\_ HQ-AWARDS

\_\_\_\_ HQ-DISTRIBUTION

\_\_\_\_ HQ-RO-GC

\_\_\_\_ HQ-COMDT

\_\_\_\_ HQ-PROCUREMENT

\_\_\_\_ HQ-RO-OWNRS

\_\_\_\_ HQ-CPO

\_\_\_\_ HQ-LOCAL MEDIA PAYMENT

\_\_\_\_ HQ-RO-PP

\_\_\_\_ HQ-DRUG

\_\_\_\_ HQ-MEDIA

\_\_\_\_ HQ-RO-S

\_\_\_\_ HQ-EMB

\_\_\_\_ HQ-PRINT

\_\_\_\_ HQ-RO-T

\_\_\_\_ HQ-OMD

\_\_\_\_ HQ-PRODUCTION CONTROL

\_\_\_\_ FT JACKSON SCH STAFF

\_\_\_\_ HQ-PB

\_\_\_\_ HQ-PROJECT OFFICER

\_\_\_\_ FT JACKSON INSTR/STU

\_\_\_\_ HQ-SECURITY

\_\_\_\_ HQ-RISC PERSONNEL

\_\_\_\_ HQ-STATS

\_\_\_\_ HQ-SALES PROMOTION

\_\_\_\_ SCHOOL LIAISON

\_\_\_\_ HQ-TRAVEL

**FINANCE AND LOGISTICS**

\_\_\_\_ HQ-CH, LOG DIV

\_\_\_\_ HQ-LOGISTICS SGT

\_\_\_\_ HQ-RML ARADS POC

\_\_\_\_ HQ-CH & SEC FAC & SVC BR

\_\_\_\_ HQ-CONTRACT SPEC

\_\_\_\_ HQ-MICO

\_\_\_\_ HQ-REALTY SPEC

\_\_\_\_ HQ-FORCE STR DIV CH

\_\_\_\_ HQ-HQ COMDT

\_\_\_\_ HQ-LOG MGT SPEC

\_\_\_\_ HQ-REQ & ORG

\_\_\_\_ HQ-HQ TRUCKMASTER

\_\_\_\_ HQ-CH, SUP & VEH BT

\_\_\_\_ HQ-PROG & TDA BR

\_\_\_\_ HQ-HQ PBO

\_\_\_\_ HQ-LOG SPEC (EQUIPMENT)

\_\_\_\_ HQ-MICO LIN (RML)

\_\_\_\_ HQ-HQ SUPPLY

\_\_\_\_ HQ-LOG SPEC (VEHICLES)

\_\_\_\_ HQ-BUDGET

\_\_\_\_ HQ-HQ UNIT HOUSING REP

**REQUESTING COMMANDER OR SUPERVISOR**

1. NAME: \_\_\_\_\_ 2. GRADE/RANK: \_\_\_\_\_ 3. TELEPHONE: \_\_\_\_\_

4. SIGNATURE: \_\_\_\_\_ 5. DATE: \_\_\_\_\_

**ARADS USER ACCESS REQUEST (BRIGADE AND BATTALION)**

(For use of this form see USAREC Pam 380-5)

**Information Required By the Privacy Act of 1974**

**Authority:** 5 USC 522A, Public Law 93-579, AR 340-21, and AR 380-19.

**Principal Purpose:** Used to identify and authorize AIS users and assign user identification (ID) codes required to access USAREC host systems.

**Routine Uses:** To assign individual's user ID code(s) and add user ID for access to USAREC host system(s).

**Disclosure:** Voluntary. Failure to furnish the information requested will result in denial of user ID(s) issuance and access to USAREC host system.

**User ID are issued to individuals based on need-to-know, job relation, and mission requirements.**

**Print or Type User Data**

1. NAME: \_\_\_\_\_ 2. GRADE/RANK: \_\_\_\_\_ 3. SSN: \_\_\_\_\_

4. ORGANIZATION: \_\_\_\_\_ 5. DUTY POSITION: \_\_\_\_\_

6. DUTY TELEPHONE: COMMERCIAL: ( ) \_\_\_\_\_ DSN: \_\_\_\_\_ 7. DATE: \_\_\_\_\_

**BRIGADE**

RECRUITING

HUMAN RESOURCES

ADVERTISING AND SALES

\_\_\_ BDE-AWARDS

\_\_\_ BDE-S1/PSNCO

\_\_\_ BDE-A&PA

\_\_\_ BDE-GC

\_\_\_ BDE-CPO LIAISON

\_\_\_ BDE-OPS

\_\_\_ BDE-HQ COMDT

\_\_\_ BDE-OWNRS

\_\_\_ BDE-SAFETY

**FINANCE AND LOGISTICS**

\_\_\_ BDE-LOG CH & CLERK/SPEC

\_\_\_ BDE-COMPTRROLLER

\_\_\_ BDE-SUPPLY

\_\_\_ BDE-REALTY SPEC

\_\_\_ BDE-MGT ANALYST

\_\_\_ BDE-UNIT HOUSING SPEC

\_\_\_ BDE-ISA COORDINATOR

\_\_\_ BDE-MANPOWER CLERK

\_\_\_ BDE-HQ COMDT BDE

\_\_\_ BDE-TRUCKMASTER

\_\_\_ BDE-PBO

**BATTALION**

RECRUITING

HUMAN RESOURCES

ADVERTISING AND SALES

\_\_\_ BN-OPS

\_\_\_ BN-S1/PSNCO

\_\_\_ BN-A&PA

\_\_\_ BN-SAFETY

**FINANCE AND LOGISTICS**

\_\_\_ BN-XO

\_\_\_ BN-HQ COMDT

\_\_\_ BN-SECRETARY

\_\_\_ BN-TRUCKMASTER

\_\_\_ BN-ISA COORDINATOR

\_\_\_ BN-PBO

\_\_\_ BN-FACILITIES MGR

\_\_\_ BN-SUPPLY

\_\_\_ BN-S1

\_\_\_ BN-UNIT HOUSING REP

**RECRUITING COMPANY**

\_\_\_ CO-CLT

**MEPS GUIDANCE COUNSELOR**

\_\_\_ ACTIVE ARMY/ARMY RESERVE

\_\_\_ NATIONAL GUARD

**REQUESTING COMMANDER OR SUPERVISOR**

1. NAME: \_\_\_\_\_ 2. GRADE/RANK: \_\_\_\_\_ 3. TELEPHONE: \_\_\_\_\_

4. SIGNATURE: \_\_\_\_\_ 5. DATE: \_\_\_\_\_





# INFORMATION SYSTEMS SECURITY PERSONNEL

(For use of this poster see USAREC Pam 380-5)



## INFORMATION SYSTEMS SECURITY PROGRAM MANAGER (ISSPM)

Barbara J. Wolfe, DSN 536-0650 or Commercial (502) 626-0650

## INFORMATION SYSTEMS SECURITY MANAGER (ISSM)

John W. Teegarden, DSN 536-0027 or Commercial (502) 626-0027, Facsimile 6-0912

## INFORMATION SYSTEMS SECURITY OFFICER (ISSO)

---

## TERMINAL AREA SECURITY OFFICER (TASO)

---

## ALTERNATE TERMINAL AREA SECURITY OFFICER (ATASO)

---

### NOTES

1. The TASO or ATASO should add the names and telephone numbers of the ISSO, TASO, and ATASO and display this poster in the TASO and ATASO area of responsibility for automated information system (AIS) security.
2. TASO and ATASO appointments must be submitted via facsimile to the ISSM listed above.
3. Individuals experiencing any known or suspected security violations, viruses, malfunctions, or other problems with an AIS or automated data processing equipment (ADPE) should notify their TASO or ATASO.