DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY RESERVE COMMAND
3800 NORTH CAMP CREEK PARKWAY SW
ATLANTA, GEORGIA 30331-5099
1 June 1996

USARC Memorandum 380-1

Security

INFORMATION SYSTEMS SECURITY

History. This is the initial printing of USARC Memorandum 380-1.

Summary. This memorandum provides policies and procedures for the implementation of security measures for classified and unclassified automated information systems (AIS) within this Headquarters, with the exception of the Reserve Component Automation System (RCAS) and the Global Command and Control System (GCCS).

Applicability. This memorandum applies to all Headquarters, U.S. Army Reserve Command, (HQ USARC) system users.

Suggested improvements. The proponent of this memorandum is the Deputy Chief of Staff for Intelligence. Users are invited to send comments and suggested improvements on DA Form 2820 (Recommended Changes to Publications and Blank Forms) directly to the proponent, ATTN: AFRC-INS.

FOR THE COMMANDER:

ZANNIE O. SMITH
Brigadier General, USA
Chief of Staff

OFFICIAL:

SIGNED
MELVIN T. LEONARD, JR.
Acting Deputy Chief of Staff,
Information Management

DISTRIBUTION: Each individual assigned or attached to HQ, U.S. Army Reserve Command

Chapter 1
General

1-1. Purpose

This memorandum prescribes procedures for preventing unauthorized access to automation equipment, material, media and documents; safeguarding against espionage, sabotage, damage and theft of information or equipment; and reducing exposure to threats that could cause a denial of service or unauthorized alteration of data. Information systems security procedures apply to all automated information systems and automated telecommunications systems, regardless of the sensitivity or classification of the information processed on these systems. This memorandum also establishes requirements and duties of personnel appointed as Terminal Area Security Officers (TASO), Alternate Terminal Area Security Officers (ATASO) and system users.

1-2. References

a. Required publications.

(1) AR 380-5 (Department of the Army Information Security Program. Cited in para 1-3c(4)

(2) AR 380-19 (Information Systems Security). Cited in paras 1-3c(2) and (4).

(3) AR 380-40 (Policy for Safeguarding and Controlling Communication Security (COMSEC) Materials (FOUO). Cited in para 1-3g.

(4) DA Pam 25-380-2 Cited in para 1-3g.

(5) TB 380-41 (Security Procedures for Safeguarding, Accounting and Supply Control of COMSEC Materials (FOUO). Cited in para 1-3g and 2-1b(4).

b. Related publications.

(1) AR 190-13 (The Army Physical Security Program).

(2) USARC Reg 25-1 (Information Resources Management Program).

(3) USARC Reg 380-2 (Information Systems Security).

(4) USARC Reg 380-3 (Safeguarding and Control of Communications Security (COMSEC) Material)

(5) USARC Memorandum 25-1 (Staff Officer's Handbook).

1-3. Responsibilities

a. Directors of coordinating, personal and special staff agencies, and Secretary for the General Staff will, within their respective agencies--

(1) Appoint a Terminal Area Security Officer/Assistant Terminal Area Security Officer (TASO/ATASO), in writing, and provide a copy of the appointment orders to each appointed individual, as well as a copy to the Information Systems Security Officer (ISSO).

(2) Accredit stand-alone, unclassified AIS.

b. Deputy Chief of Staff, Information Management will issue appointment letters for the Information Systems Security Officer (ISSO) and the Network Security Officer (NSO).

c**. Information Systems Security Manager (ISSM).** Assigned within the Deputy Chief of Staff, Intelligence, the ISSM will--

(1) Establish and implement an Army Information Systems Security Program (AISSP) for all telecommunications and automated information systems.

(2) Ensure networks are accredited by the appropriate designated accreditation authority (DAA) to operate in accordance with AR 380-19. Periodically review the status of networks to ascertain that changes have not occurred which affect security and negate the accreditation.

(3) Ensure appointment letters are issued for the USARC local area networks as follows:

(a) The DCSIM will issue appointment letters to the ISSO and NSO.

(b) Each director/chief will issue appointment letters to their Terminal Area Security Officers (TASOs).

(4) Report security incidents and technical vulnerabilities in accordance with AR 380-19 and AR 380-5.

(5) Review threat and vulnerability assessments to properly assess risks and determine effective measures to minimize such risks.

(6) Distribute current USARC personnel security clearance and access roster to security managers.

(7) Oversee the execution of the Information Systems Security training and awareness program. Ensure TASOs brief all personnel of their security responsibilities and appropriate security procedures within 30 days following assignment.

(8) Schedule and supervise the inspection of the cable paths.

(9) Establish and manage the Command Information Systems Security (ISS) Program, to include defining the ISS personnel structure and directing the appointment of ISS personnel.

(10) Ensure users operate and maintain information systems according to all applicable regulations and this memorandum.

d. Information Systems Security Officer (ISSO). Assigned within the Deputy Chief of Staff, Information Management (DCSIM), the ISSO is responsible for all aspects of security (personnel, physical, communications, emanation, hardware, software, and procedures) for Headquarters, USARC information systems. The ISSO will perform the following functions for all HQ USARC networks:

(1) Prepare and maintain network accreditation documents and initiate re-accreditation when changes affecting security have occurred.

(2) Ensure users operate and maintain information systems according to all applicable regulations and this memorandum.

(3) Prepare, distribute and maintain plans, instruction guidance, and standing operating procedures regarding the security of system operations.

(4) Compile and maintain the Network Control Center (NCC) access roster and provide a copy to the ISSM and NCC personnel.

(5) Maintain a current list of TASO appointments.

(6) Approve issuance, control, and account for NCC security badge access.

(7) Provide ISS briefings for TASOs and users.

(8) Direct the suspension of support or service to any system user not adhering to the regulations and procedures in effect.

(9) Conduct threat and vulnerability assessments to properly assess risks and determine effective measures to minimize such risks.

(10) Approve the use of required non-standard software on USARC personal computers (PCs) or network.

(11) Inspect all wires and network cables for tampering on a regular basis. If necessary, the inspection may be of the conduit that holds the wires or cables.

(12) Perform the duties of the Network Security Officer (NSO) in his/her absence.

e**. Network Security Officer (NSO).** Assigned within the Deputy Chief of Staff, Information Management, the NSO is responsible for all aspects of security (personnel, physical, communications, emanation, hardware, software and procedures) within the NCC. The NSO will--

(1) Ensure security measures and procedures fully support the security and integrity of the network and comply with applicable directives.

(2) Establish procedures to control network access and connectivity. Conduct periodic review of system audit logs.

(3) Conduct reviews of threats to and vulnerabilities of the network. Report immediately to the ISSO any system failure that could lead to unauthorized disclosure or attempts to gain unauthorized access to sensitive information.

(4) Review and evaluate, in conjunction with the ISSO, the security impact of changes to the network, including interfaces with other networks or systems.

(5) Suspend support or service to any system user not adhering to the regulations and procedures in effect.

(6) Ensure users operate and maintain information systems according to all applicable regulations and this memorandum.

(7) Ensure NCC personnel properly safeguard COMSEC material located within the NCC.

(8) Generate passwords and user identification codes (user IDs). Add the user to the network with appropriate services.

(9) Perform the ISSO duties in the absence of the ISSO.

f. Terminal Area Security Officers (TASO)/Assistant Terminal Area Security Officer (ATASO). Assigned

within all directorates, coordinating and special staff agencies and Secretary for the General Staff, the TASO is responsible for all aspects of security (personnel, physical, communications, emanation, hardware, software and procedures) within their assigned area. Each director/chief will appoint a TASO/ATASO in writing and provide a copy of the appointment orders to both the individual and the ISSO. Continuity of TASO/ATASO appointments and training is the responsibility of the using agency. The TASO/ATASO will--

(1) Approve access of authorized users to the networks.

(2) Verify each user's identity, need-to-know, level of clearance, and authorized access.

(3) Request the suspension of support or service to any system user, within their organization, not adhering to the regulations and procedures in effect.

(4) Ensure users operate and maintain information systems according to all applicable regulations and this memorandum.

(5) Distribute plans, instruction guidance and standing operating procedures regarding the security of system operations.

(6) Report to the ISSO any attempt to gain unauthorized access to information and any system failure or suspected defect or vulnerability that could lead to unauthorized disclosure.

(7) Ensure preparation and approval of accreditation documentation for any stand-alone systems, within their functional area. Maintain accreditation documentation on file.

(8) Prepare and submit requests for all passwords and user IDs to the NSO on AFRC Form 48-R (Classified Network Password Request Form). (See para 2-3a.)

(9) Give initial ISS briefing to each user (within 30 days following assignment) and ensure user understands and signs AFRC Form 47-R (Information Systems Security Briefing for Users of the U.S. Army Reserve Command Local Area Networks). (See para 2-3c.)

(10) Provide periodic ISS training and awareness briefings to each user.

(11) Ensure users log off the network, and secure the removable disk, if appropriate, whenever the system is left unattended.

(12) Report all USARC network problems to the USARC Help Desk.

(13) Perform end-of-day security checks in assigned area of responsibility.

(14) Issue instructions specifying security requirements and operating procedures.

(15) Ensure each user has a current copy of this memorandum and follows the guidance herein.

(16) Conduct periodic checks of their area of responsibility to ensure that users follow access and authorization procedures.

(17) Ensure local office procedures exist to provide formal accountability of all PCs.

(18) Ensure all users with access to the USARC classified local area network (LAN) are debriefed and turn-in their classified SyQuest cartridges to the NSO upon reassignment.

g. Communications Security (COMSEC) Officer. The COMSEC Officer and alternate are responsible for the accountability of all COMSEC materials within the Headquarters, USARC. Specific duties are described in the USARC Regulation 380-3, AR 380-40, and TB 380-41 series. The COMSEC Officer and alternate will control and distribute cryptographic keys according to policies and procedures in USARC Regulation 380-3, AR 380-40, and DA Pamphlet 25-380-2.

h. Network Control Center (NCC) personnel. The NCC personnel will, as a minimum--

(1) Restrict NCC access to authorized personnel only.

(2) Ensure all visitors sign in and are escorted, as required, while they are within the facility.

i. System users.

(1) All users will, as a minimum--

(a) Control their user ID and password. Users will not share passwords. Users will maintain, store, and destroy completed Parts B of USARC Form 48-R in accordance with AR 380-5.

(b) Immediately report to their TASO/ATASO any data that may inadvertently appear on the screen that cannot be identified or any data that can be identified, but for which access has not been authorized.

(c) Immediately report compromised passwords to the TASO/ATASO.

(d) Immediately report to the TASO/ATASO any attempt to gain unauthorized access to information, any system failure or any suspected defect or vulnerability which could lead to unauthorized disclosure.

(2) In addition, all users of classified PCs will, as a minimum--

(a) At no time leave a PC with the classified SyQuest cartridge installed unattended in the logged-on mode. If a user must leave a PC with the classified cartridge installed, they will log off and secure the removable disk in a GSA-approved security container to prevent unauthorized use of the PC, and to prevent persons without a need-to-know from viewing sensitive or classified data.

(b) Return classified SyQuest cartridges to the NSO upon reassignment.

j. USARC Facility Manager. The USARC Facility Manager will immediately notify the ISSO or NSO when the building security system is turned off or is non-functioning for any reason or period of time.

Chapter 2
Security

2-1. Physical security

a. Building access. All HQ USARC buildings are considered limited access areas. Personnel will carry and properly display a building access badge or be escorted, as required by USARC Memorandum 25-1.

b. NCC.

(1) The NCC is designated as a restricted area in accordance with AR 190-13. The NCC personnel will post a clearly visible sign outside the NCC with the following verbiage:

RESTRICTED AREA

THIS AREA HAS BEEN DECLARED A RESTRICTED AREA BY AUTHORITY OF THE COMMANDING GENERAL IN ACCORDANCE WITH THE PROVISIONS OF THE DIRECTIVE ISSUED BY THE SECRETARY OF DEFENSE ON 20 AUGUST 1954, PURSUANT TO THE PROVISIONS OF SECTION 21, INTERNATIONAL SECURITY ACT OF 1950, UNAUTHORIZED ENTRY IS PROHIBITED. ALL PERSONS ENTERING HEREIN ARE LIABLE TO SEARCH. PHOTOGRAPHING OR MAKING NOTES, DRAWINGS, MAPS OR GRAPHIC REPRESENTATIONS OF THIS AREA OR ITS ACTIVITIES ARE PROHIBITED UNLESS SPECIFICALLY AUTHORIZED BY THE COMMANDER. ANY SUCH MATERIAL FOUND IN THE POSSESSION OF UNAUTHORIZED PERSONS WILL BE CONFISCATED.

(2) The NCC personnel will post a copy of the NCC access roster in the NCC.

(3) A USARC badge specifically coded for NCC access is requisite for badge entry to the NCC.

(4) All visitors, other than those identified on the access roster, must contact NCC personnel for entry, sign in on DA Form 1999-R (Restricted Area Visitor Register), and be escorted while in the NCC. NCC personnel will use DA Form 1999-R to record the arrival and departure of all personnel not authorized unrestricted access to the area. (A copy of DA Form 1999-R is in TB 380-41 for local reproduction.)

c. General physical security. Where possible, users should place PCs in such a way as to preclude casual viewing by unauthorized personnel.

2-2. Security incidents

Immediately report to the ISSO and TASO/ATASO, all actual or potential security incidents such as--

a. Unexplained output received (receipt of information not requested).

b. Abnormal system response to a user's input.

c. Inconsistent or incomplete security markings on output.

d. System by-product material or output from a previous user remaining uncontrolled in the area.

e. Unattended device signed on and connected to the system.

f. Unknown or unauthorized personnel using the system.

g. Any event or occurrence that is an exception to normal operating procedures.

h. Unattended classified material or classified SyQuest cartridges.

2-3. Passwords

a. Classified. The TASO will request classified passwords by completing the framed portion of AFRC Form 48-R (Classified Network Password Request Form), Part A, and submitting it to the NSO. Upon receipt of a valid AFRC Form 48-R, the NSO will obtain a randomly generated password and network user account. When notified by the NSO, the user will pick up the completed Password Request Form, Part B of AFRC Form 48-R, within 3 weeks of the processed date. The NSO will have the user account deleted from the system if the password is not picked up within the stated timeframe. The user must sign and date the AFRC Form 48-R to acknowledge acceptance of the user ID, password, classified cartridge, and responsibilities for system security. Passwords for the classified network expire 6 months from date of issue. Users must contact the NSO for a new password. A blank copy of AFRC Form 48-R is at the back of this memorandum for local reproduction.

b. Unclassified. The TASO may request unclassified passwords via electronic mail to the NSO. The NSO will obtain a randomly generated password and network user account, and forward the requested information to the TASO. The first time the user logs on to the unclassified network, they will be prompted to change their password. Thereafter, the user will change passwords for the unclassified network annually. The network will prompt the user when the change is required. The password must be a minimum of six random alpha characters.

c. Security briefing.

(1) At the time of password issuance, the TASO will brief individual users on--

(a) Password classification and exclusiveness.

(b) Measures to safeguard system passwords.

(c) The prohibition against disclosure to other personnel.

(d) The requirement to immediately inform a TASO or the ISSO of password misuse or compromise.

(2) Following the briefing, the TASO must have the user read and sign AFRC Form 47-R. A blank copy of the form is at the back of this memorandum for local reproduction.

2-4. Software
Appendix Q, paragraphs Q-8 and Q-9 of USARC Memorandum 25-1 addresses hardware and software policy. Individuals will not load other software to the PC or network without the written approval of the ISSO, in conjunction with the NSO. Users may submit requests for exception, fully justified in writing, through the TASO to the ISSO. Violations will be reported by the TASO to the appropriate director or office chief and the Chief of Staff.

2-5. Compliance
Each USARC employee is responsible for complying with policies and procedures in this memorandum. Any persons observing violations of security directives will report them immediately to the appropriate authority for action.

Glossary

Section I
Abbreviations

AIS ..... automated information system(s)
AISSP ..... Army Information Systems Security Program
ATASO ..... Alternate Terminal Area Security Officer
COMSEC .... communications security
DAA ..... designated accreditation authority
ISS ..... Information Systems Security
ISSM ..... Information Systems Security Manager
ISSO ..... Information Systems Security Officer
PC ..... personal computer
TAIS ..... Telecommunications Automated Information Systems
TASO ..... Terminal Area Security Officer
NCC ..... Network Control Center
NSO ..... Network Security Officer

Section II
Terms

Accreditation
The formal declaration by the DAA that the AIS is approved to operate in a particular security mode using a prescribed set of safeguards.

Automated information system
Computer hardware, software and/or firmware used to collect, create, communicate, disseminate, process, store and/or control data or information. Included are computers, word processing systems, networks, or other electronic information handling systems, and associated equipment.

Automated information systems security
Synonymous with computer security. Measures and controls that protect an AIS against denial of service and unauthorized (accidental or intentional) disclosure, modification, or destruction of AISs and data.

Army Information Systems Security Program
A unified approach to protecting classified and unclassified-sensitive information while in TAIS or non-communications emitters, during the development, acquisition, training, deployment, operations, maintenance, and disposition of the TAIS or non-communications emitter.

Compromise
A violation of the security policy of a system such that unauthorized disclosure of sensitive information may have occurred.

Designated accreditation authority
The official who has the authority to decide on accepting the security safeguards prescribed for an AIS or that official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards.

Sensitive information
Any information whose loss, misuse, modification, or unauthorized access could affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code; but that has not been specifically authorized under criteria established by an Executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy.