SECURITY MANAGER'S HANDBOOK

Headquarters, United States Army Recruiting Command
1307 3rd Avenue
Fort Knox, Kentucky 40121-2726
June 2003

This pamphlet is published by the United States Army Recruiting Command ~~Support Brigade~~, Security Office ~~Division~~, Fort Knox, Kentucky. It is intended to be used as an aid to security managers. This pamphlet does not establish policy. However, it provides a ready source of information for security program issues that may confront a security manager. It is suggestive in format and is not all inclusive. Each activity may have specific requirements that are quite varied or may not be provided for in this pamphlet. Further improvements, changes, and additions may be developed by individual security managers to meet the needs of their organization. The pamphlet is divided into two sections: Intelligence-related security programs (chaps 1 through 15) and physical security programs (chaps 16 through 20).

Comments and suggestions regarding this pamphlet are solicited and should be directed to the United States Army Recruiting Command ~~Support Brigade~~, Security Office ~~Division~~.

Telephone numbers for the Security Office ~~Division~~ are:

DSN 536-0238
Commercial ..... (502) 626-0238
FAX ..... (502) 626-0918

Telephone number for Information Systems (ADP) ..... (502) 626-0027
Telephone number for the Fort Knox 902nd MI Group ..... DSN 464-7647
Telephone number for direct reporting of SAEDA is USAINSCOM, Fort Meade, MD ..... (800) CALLSPY

Headquarters
United States Army Recruiting Command
Fort Knox, Kentucky 40121-2726
15 May 2000

***USAREC Pamphlet 380-4**

Security

Security Manager's Handbook

For the Commander:

WANDA E. WILSON
Colonel, GS
Chief of Staff

Official:

ROGER H. BALABAN
Chief Information Officer

History. This UPDATE printing publishes a new Change 2, dated 3 June 2003. The strikethrough and underscore method has been used to highlight changes and figure 15-6 has been deleted.

Summary. To provide a handy reference document for security managers that encompasses the major security issues, some of which may not be applicable to all recruiting activities. Information within this pamphlet does not supplement Army regulations, USAREC regulations, other published policies or supplements, and should not be used in lieu of either. It is intended as a guide which can be used in conjunction with appropriate publications. It contains basic information found in AR 380-5, AR 381-12, AR 380-19, AR 380-67, AR 190-13, AR 190-40, AR 25-55, and other reference materials.

Applicability. All USAREC security managers are encouraged to maintain a copy of this pamphlet. This pamphlet is intended to remain with the unit. Procedures used by a supporting installation may not be, in all cases, the same as contained in this pamphlet. When differences occur, follow written Army regulations, USAREC publications, and/or supporting installation and activity procedures.

Proponent and exception authority. The proponent of this pamphlet is the ~~Commander, United States Army Recruiting Support Brigade~~ Office of the Chief of Staff. The proponent has the authority to approve exceptions to this pamphlet that are consistent with controlling law and regulation. Proponent may delegate the approval authority, in writing, to the ~~executive officer within the proponent agency in the grade of lieutenant colonel~~ Command Security Officer.

Suggested improvements. ~~The proponent agency of this pamphlet is the Commander, United States Army Recruiting Support Brigade.~~ Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to ~~Cdr, RS Bde (RCRS-SEC),~~ HQ USAREC (RCCS-SEC), 1307 3rd Avenue, Fort Knox, KY 40121-2726.

Distribution. Special. One each security manager. This pamphlet is also available electronically on the USAREC Intranet Homepage at http://home.usarec.army.mil.

Contents (Listed by paragraph)

---

*This pamphlet supersedes USAREC Pamphlet 380-4, 21 April 1997.

Chapter 1
Introduction

1-1. Purpose

a. This pamphlet contains no classified information. All security classification markings, declassification, downgrading instructions, and warning notices are for illustrative purposes only.

~~b. It contains one For Official Use Only (FOUO) section (fig 15-6).~~

be. It provides general guidance to assist security managers (SMs) in the performance of duties as required by security publications found in appendix A.

1-2. References

a. For required and related publications and referenced forms see appendix A.

b. SMs are not expected to memorize or retain the large volume of information contained in the numerous security regulations and documents. SMs need to familiarize themselves with which documents contain the information they may require on a particular subject and where it can be found in the document.

1-3. Explanation of abbreviations

Abbreviations used in this pamphlet are explained in the glossary.

1-4. Commanders' responsibilities

a. Commanders at all echelons have the responsibility for effective security programs and implementation of security education in the unit or organization.

b. They are directly responsible for implementing and enforcing security policies and procedures; initiating and supervising measures or instructions necessary to ensure continual protection of classified information; assuring that persons requiring access to classified information are properly cleared; and continually assessing the individual trustworthiness of personnel who possess a security clearance.

c. A commander may delegate authority to perform local security functions, but not the responsibility to do so. Security is always the responsibility of the commander.

1-5. SM responsibilities

The SM is the commanderís authorized representative, responsible for the establishment and administration of an effective security program. The SM should be appointed in writing and should be in the grade of GS-7 or E-7, or above. The SMís duties include:

a. Advising and representing the commander or supervisor on matters related to security.

b. Establishing and implementing an effective security education program.

c. Establishing procedures for assuring that all persons handling classified material are properly cleared and have a need to know.

d. Advising and assisting officials holding classified material on classification problems and the development of classification guidance.

e. Ensuring that classification guides for classified plans, programs, and projects are created early, reviewed, updated, and made available to all persons concerned.

f. Conducting periodic reviews of classified holdings within the activity to ensure proper classification.

g. Reviewing classified holdings to reduce unneeded classified material, by declassification, destruction, or retirement, and overseeing annual cleanout day.

h. Supervising and conducting security inspections and spot checks and notifying the commander regarding compliance with security directives.

i. Assisting and advising the commander in matters pertaining to the enforcement of regulations governing the dissemination, reproduction, transmission, safeguarding, and destruction of classified material.

j. Being the single point of contact on security matters for his or her unit or activity.

k. Establishing effective and comprehensive standing operating procedures (SOPs) for the activity or unit. A successful security program is accomplished through cooperation between the commander and the SM. The commander needs to appoint an SM with the necessary prerequisites to perform the above tasks and provide them sufficient time and manning to perform the job properly. SMs should provide the commander with timely and professional advice concerning the security posture of the unit and make recommendations to solve or eliminate security problems. Enforcement of established security policies is the responsibility of the commander (AR 380-5).

Chapter 2
Security Education and Training

2-1. Security education

a. The key to a successful security program is a well-informed, trained, and educated SM.

b. The tools of a successful SM are training and education. The program stresses the objectives of the protection of classified information. Ensure that your program is hands on and that all training is documented in writing.

c. All personnel authorized or expected to be authorized access to classified information must receive instruction in accordance with AR 380-5. Exercise care to ensure that the instruction does not evolve into a perfunctory compliance with formal requirements without achieving the real goals of the program. Having individuals read large compilations of security regulations and obtaining a signature is neither adequate nor acceptable.

2-2. Initial security briefings

a. All individuals, regardless of their security clearance status, receive an initial security orientation upon assignment or employment by any element of this command. The SM records receipt of initial security orientation and refresher briefings. As a minimum, design briefings to:

(1) Advise personnel of the adverse effects to national security which could result from unauthorized disclosure and advise them of their personal, moral, and legal responsibility to protect classified information within their knowledge, possession, or control.

(2) Indoctrinate personnel in the principles, criteria, and procedures for the classification, downgrading, declassification, marking, and dissemination of information as prescribed in the Army regulations, and alert them to the strict prohibitions on improper use and abuse of the classification system.

(3) Familiarize personnel with procedures for challenging classification decisions believed to be improper.

(4) Familiarize personnel with the security requirements of their particular assignment.

(5) Inform personnel about techniques employed by foreign intelligence activities in attempting to obtain classified information, and their responsibility to report such attempts or related or possibly related incidents (see AR 381-12 and AR 530-1).

(6) Advise personnel about penalties for engaging in espionage activities.

(7) Advise personnel of the strict prohibition against discussing classified information over an unsecured telephone or in any other manner that permits interception by unauthorized personnel.

(8) Inform personnel of administrative sanctions that may be taken against personnel who knowingly or willfully disregard the provisions of AR 380-5.

(9) Instruct personnel that individuals having knowledge, possession, or control of classified material must determine, before disseminating such material, that the prospective recipient is cleared for access, needs the information in order to perform his or her official duties, and can properly protect (or store) the material.

b. Advise personnel of the requirements to report such matters as:

(1) Physical security deficiencies.

(2) Possible loss or compromise of classified material.

(3) Information that could reflect adversely on the trustworthiness of an individual who has access to classified information.

(4) For persons who will have access to classified intelligence information, explain in general terms the intelligence mission of the US Army and the reasons why intelligence information is sensitive. (AR 380-5.) See figure 2-1.

2-3. Refresher briefings

a. SMs must provide, as a minimum, annual security training for personnel having continued access to classified information or who can be expected to handle classified information. Attendance at such training must be annotated.

b. Annual attendance of personnel at a security education presentation is not considered fulfillment of this requirement, nor will merely reading regulations and signing a statement that an individual has read and understands.

c. Instruction must provide effective education of personnel in the subjects listed above and be tailored to suit the nature of the individualís particular involvement with the Information Security Program.

2-4. Subversion and Espionage Directed Against the US Army training

a. All Department of Defense (DOD) affiliated personnel must receive an initial briefing and biennial Subversion and Espionage Directed Against the US Army (SAEDA) training. Counterintelligence personnel or the SM will present this training. Subject matter requirements are determined in AR 381-12. SMs can receive assistance in preparing and presenting SAEDA instruction from the supporting military intelligence element and the command SM.

b. Biennial SAEDA briefing requirements are not considered fulfilled unless terrorism countermeasures are included as part of the overall briefing.

c. SMs must make every effort to prepare current, interesting, and relevant presentations. Individuals who are especially vulnerable to foreign intelligence agent approaches by virtue of their position, travel, duties, or activities must receive a special SAEDA briefing. Specific situations requiring a special SAEDA briefing are given in AR 381-12 (see fig 2-2).

2-5. Foreign travel briefings

Individuals having access to classified material are targets for foreign intelligence agents when traveling to foreign countries or to symposiums or meetings within the continental United States where they may come into contact with foreigners from special concern countries. (See figs 2-3 through 2-6.)

2-6. Terrorism briefings

All Department of the Army (DA) personnel, civilian and military, traveling outside continental United States (OCONUS) for any reason, official or personal, must receive the applicable antiterrorism briefing as required by AR 525-13.

2-7. US Army Intelligence activities training

a. AR 381-10 applies to all intelligence units that support unified or specific commands, intelligence staff offices supporting military commanders at all echelons, S2 or G2, and other DA military personnel and civilian employees when they engage in authorized intelligence activities.

b. Personnel in a position to collect or store information on US and non-US persons and organizations must receive an initial briefing and annual familiarization on the intent and restrictions outlined in AR 381-10. (Also see figs 2-7 through 2-9.)

The American people have placed a special trust and confidence in each of us to protect national security secrets. We have taken an oath to faithfully discharge our duties as military or civilian employees - an oath that is violated when unauthorized disclosure of classified information is made. Each of us recognizes that certain matters require confidentiality in order to carry out diplomacy with friends and foes - peace depends on it.

a. Nuclear dangers, terrorism, and aggression demand that we gather intelligence information about these dangers and we must protect our sources if we are to continue to receive such information.

b. The constitution guarantees each of us the right to voice our own opinions - yes even criticizing our Government if we so desire. But we do not have the right to damage our country by careless security procedures that allows the disclosure of sensitive and classified information.

c. Be particularly circumspect in approaches which may be made offering social companionship, especially of a sexual nature. Many of these persons are ìplantsî of designated country intelligence agencies and will offer themselves attractively for the purpose of getting you in a compromising situation which will be followed by blackmail threat to force your cooperation in intelligence activities. Under no circumstances should you seek or accept this kind of social companionship in a Communist or special concern country. The intelligence services are fully aware of the possibilities inherent in human frailties, and will capitalize immediately upon any indication of immoral or indiscreet behavior of American travelers. Even when failing to detect a vulnerability, agents have attempted entrapment of innocent travelers.

d. For this reason, you should maintain the highest level of personal behavior at all times, avoid long walks at night alone, and endeavor to always be in the company of someone you can trust. Be especially careful to stay well within your capacity for alcohol so as not to weaken your defense or lose your self-control.

e. Do not accept from anyone (including friends, relatives, or professional contacts) letters, photographs, packages, or any other material to be smuggled out of the country or carried in your effects when you depart. Be firm in your denials in these matters, as such requests may be acts of intelligence provocation to entrap you.

f. Bear in mind that there are many political, cultural, and legal differences between the U.S. and special concern countries. Actions which are innocent or, at worst, carry wrist-slapping penalties in the U.S., are often considered serious offenses.

g. The protection of national defense information is the responsibility of each individual who possesses or has knowledge of such information regardless of how it was obtained. Security regulations cannot guarantee absolute protection and cannot be written to cover all conceivable situations. Therefore, we must use common sense and a logical approach when applying security procedures and interpreting existing directives.

h. Access to classified information is based on an appropriate security clearance and a need-to-know. No one has the right to classified information solely by virtue of rank or position.

i. During face-to-face contact be certain that classified information is being discussed only with persons who have a proper security clearance, a need-to-know, and that they understand that the information is classified and the degree of classification. Collecting, obtaining, recording, or removing any classified material for personal use is prohibited.

j. Under no circumstances will classified information be given or released to foreign nationals or foreign governments unless authorized under the national disclosure policy. Contact your security manager for further guidance.

k. If you have knowledge of the actual or possible compromise of classified information, immediately report the circumstances to your supervisor, security manager, and/or commander. The security manager must also contact your security manager or the USAREC security manager at DSN 536-0238 or commercial (502) 626-0238. All Department of the Army personnel are responsible for reporting such incidents.

l. Persons responsible for any unauthorized removals or disclosures are subject to severe sanctions. This may include action under the Uniform Code of Military Justice or other federal statutes and, when warranted, referral for criminal prosecution.

Figure 2-1. Sample of initial security briefing

m. Unclassified information that does not appear to have any significant value from an intelligence point of view may be of great value to foreign intelligence agents. Donít discuss information relating to unit training, mobilization, exercise, equipment, unit readiness, etc., outside the work area.

n. Public disclosure of classified information by non-Government sources (i.e., a newspaper article, CNN, etc.,) must be distinguished from Government confirmation. Confirmation of such information by a Government employee greatly increases the intelligence value of media speculation.

o. Reproduction of classified material is prohibited unless specifically approved by the security manager and the copy machine has been approved for copying classified information. A notice should be posted on or near the reproduction equipment to verify use for classified reproduction.

p. Classified information will only be processed on computers officially accredited, in writing, for the processing of classified information. Contact the USAREC security manager for further guidance.

q. Except as authorized by Army regulations, Department of the Army civilians and military may not engage in electronic surveillance of any kind. Do not discuss classified information over an unsecured telephone and donít try to be clever and talk around classified information over the telephone. Use only secure voice systems authorized to transmit classified information when it is absolutely essential to discuss classified information telephonically.

r. If you suspect or discover a technical surveillance device, take no action other than to notify the local 902nd Military Intelligence Group or the USAREC security manager.

s. All US Government furnished desks, cabinets, lockers, or other containers within Government facilities are for official use only and subject to search for improperly secured classified documents and/or materials. All such items will remain unlocked or if locked, duplicate keys or combinations will be provided to the security manager.

t. Remember, you are the prime target of the foreign intelligence agent. These agents will attempt to identify and exploit any character weaknesses that you may have (i.e., financial problems). If you suspect such an approach has been made, you are required to report your suspicions to the 902nd Military Intelligence Group or the USAREC security manager. Under no circumstances should you attempt on your own to pursue the development of a relationship with a person you suspect to be connected with foreign intelligence services.

u. Family members should also be aware of methods used by foreign intelligence agents to recruit and/or obtain military information and how to report an incident.

THINK SECURITY!

Figure 2-1. Sample of initial security briefing (Continued)

Due to the nature of the mission of Fort Knox, USAREC, and tenant elements stationed here, espionage is an ever present threat. Historically, foreign intelligence agents (FIAs) are more aggressive and most effective during periods of peace and relaxed military tensions. Many foreign powers choose these periods to step up the intensity of their intelligence gathering operations because people in their target countries see them as friends.

a. Each of us possesses information of value to FIAs. Therefore, we need to be acquainted with methods used by FIAs to obtain information and our responsibility to report any actual or suspected recruitment. First, however, it is important to understand each element of Subversion and Espionage Directed Against the US Army.

(1) Subversion. The attempt by an individual or group to undermine our faith and allegiance in our Government, our nation, or the American form of government and life.

(2) Espionage. The practice of obtaining, transmitting, or receiving information concerning national defense, technology, or security with the intent of assisting foreign powers and other disruptive elements.

(3) Directed Against the US Army. Self-explanatory.

b. Human intelligence.

(1) Members of this countryís Armed Forces, civilian employees, and family members are prime targets for espionage by foreign intelligence services (FIS). For that reason, it is important to remember that we are all potentially subject to approach by FIAs regardless of our location, rank or grade, or job.

(2) On 25 December 1991, the Soviet Union ceased to exist as we have known it for the past 40 plus years. The former Soviet Unionís implementation of glasnost and peristrokia, the subsequent breakup of the USSR, the Warsaw pact, and the economic problems found in these countries has increased, not decreased, the espionage threat.

(3) We have also witnessed a significant increase over previous decades in the number of citizens being convicted on charges of espionage. Greed for money, disgruntlement, and adventure ranked high as motivating factors. FIAs will continue to attempt to cultivate sources with actual or potential access to valuable information. Although we have yet to see what espionage attempts will surface in the future, it is certain that the threat posed by FIS is extensive. ìCoopteesî and all others who assist the FIS add to this threat because they are much harder to uncover.

(4) The flow of technology to foreign countries has increased significantly in recent years, to a large measure, due to the influence of detente. Foreign countries have sizable delegations within the US who have considerable freedom of movement in which they attempt to acquire technology in all stages of development.

(5) The former Soviets, their allies, and other FIS rely heavily on the cooperation of representatives from their news services, commerce - including the approximately 20,000 merchant seaman who visit US ports each year, accredited personnel, educational, technical, and scientific institutes, and cultural exchanges for information.

(6) When considering the threat one must consider not only the numbers of intelligence agents but also, and equally important, the openness of our society. When we see information that we know to be classified in newspapers or other open media, we sometimes question the need to further protect that information and lose faith in our security procedures.

(7) Public disclosure of classified information by non-Government sources must be distinguished from Government confirmation. Verification by a Government source greatly increases the intelligence value of media speculation. Remember: Public disclosure does not relieve us from our responsibility to continue protecting the information as classified.

(8) When an individual in a position of trust and responsibility deliberately and willingly discloses classified information to a person or organization not authorized access to that information a deliberate security violation has occurred. Such a violation is punishable by a $10,000 fine, 10 years in prison, or both. Other higher penalties have been and can be imposed.

Figure 2-2. Sample SAEDA briefing

(9) Making maximum use of western technology obtained through either legitimate open sources or illicit means, foreign countries can concentrate their assets on other activities. If they can purchase or steal technology, they can then divert resources into other critical areas with direct military applications, such as missile or tank development. For this reason, it is imperative that sensitive information in every phase of research and development is protected.

c. Open sources.

(1) Intelligence information gained by various means and agents employ many avenues to gather classified and sensitive information. They obtain approximately 90 percent of their information from legal or open sources such as periodicals, libraries, and newspapers. Trained personnel review and analyze trade journals, magazines, newspapers, etc., and compile the information which frequently provides them with quite an accurate picture of US defense spending on research, deployments, and resources.

(2) They have also been known to approach authors to solicit information or attempt to obtain invitation to conferences and seminars where prominent authors and scientists are in attendance. Our open society affords agents tremendous opportunity to legally obtain information critical to developing their military and economy. Unfortunately, this is one time democracy works to their advantage and not ours.

d. Signals intelligence.

(1) Some foreign countries conduct extensive signals intelligence gathering efforts, continually attempting to glean information by monitoring our telephones and radio traffic. Telephones provide an ideal pathway for information. Cellular telephones and our Defense Switched Network which uses microwave relay, is one of the greatest threats to security. Do not use an unsecured telephone to discuss classified information.

(2) Every telephone contains a minimum of two microphones. Either one of them can be easily connected so that all conversations taking place within the room can be broadcast and monitored from another location without the use of telephone lines. Multiple-line call telephones compound the risk because these have spare wires that can be used to pass information to an unknown listener.

(3) To prevent this from happening, ensure that all buttons on your telephones are in the up position when not in use. Monitoring can occur from the ground, ships, or airborne platforms. Commercial and research vessels frequently dock in northwest ports and commercial airlines fly into several northwest cities on a regular basis, all with a monitoring capability.

e. Espionage.

(1) To fill in the 10 percent critical gap, intelligence agents rely almost exclusively upon the human source, targeting against that information which is not available through open sources. This type of collection effort is usually expensive, time-consuming, and involves potential political embarrassment for the sponsoring government should its activities be discovered. However, the value of the desired information normally justifies the cost and risk.

(2) Agents will use all available means to coerce, trick, deceive, or pressure you into releasing sensitive or classified national defense information. Methods of entrapment, such as blackmail, friendship, and physical threats are standard methods of operation used by intelligence agents. Although their initial requests may be for unclassified and seemingly innocent items such as phone books and personnel rosters, demands for classified information will inevitably follow.

(3) In an espionage operation, the agent will find the person who is weak, careless, or who will willingly provide intelligence information for either monetary or political reasons. Another way agents obtain information is through an individual whose cooperation is solicited through the use of blackmail: The chronic gambler, the alcoholic, the sexual pervert, and the unfaithful husband or wife. Severe pressure can be brought to bear on these individuals through blackmail! Report each potential problem - only you can stop the threat to national security when a blackmail attempt confronts you.

Figure 2-2. Sample SAEDA briefing (Continued)

(4) Another technique used is misrepresentation of status, or the ìFalse Flagî approach where agents attempt to pass themselves off as members of a US agency or friendly government.

(5) We can unwittingly provide intelligence information through casual conversations which can take place in the snack bar, on a shuttle bus, McDonaldís, or in a bar. Intelligence collected by this method is evaluated as extremely reliable because the source is unaware of what is happening. What better way is there to obtain cheap, reliable classified information? Never discuss classified information away from the workplace or in an uncleared area.

(6) As you can see, intelligence agents have a workable formula for successful operations. They make use of typical American characteristics, that of being friendly, outgoing, and willing to accept people at face value. This makes us extremely vulnerable to deception and possible exploitation. Remember: Agents are talent scouts who look at every person they meet as a potential client.

f. Recruitment.

(1) The intelligence agent asks himself, ìWhich one of them has or will have the information I need?î ìHow can I coerce him or her to cooperate?î ìHow much would it take to buy their cooperation?î If you are approached you have been carefully targeted and selected - the agent has already identified what he or she considers to be ìyour unique weakness.î

(2) You wonít be approached at a party by someone thrusting a martini into your hand and probing you with questions about classified or sensitive material you handle. They arenít that stupid and they donít assume that you are either. They will gradually try to assess your potential before they make a move. Agents use many avenues of approach. The most basic is ideological, just to see where your thinking lies. They may try to find individuals who are sympathetic to the international aims of their country, has family ties, or political causes to the right or left. Agents also look for individuals who are sympathetic to various ethnic or racial movements.

(3) The individual considered most damaging and dangerous to national security is the US citizen who isnít recruited. This individual willingly provides information to foreign governments due to some personal motivation. No pressure is brought to bear on this person, no initial recruitment takes place. These individuals may not outwardly exhibit any bad character habits and, as a result, are harder to detect and neutralize.

g. Defensive measures against espionage.

(1) Knowledge is the best defense against espionage. Aggressive unit security education programs help personnel recognize warning signs.

(2) A secondary defense is the personnel background investigation conducted by various intelligence or investigative agencies. Most of us have been a part of one. Cooperate when agents come around, show their badge and credentials, and ask about a person in need of a security clearance. Take the time and effort to think about this personís character. Does it lend itself to blackmail? Is the individual a chronic gambler or alcoholic?

(3) Does this person leave the safe open? Does the individual have more money than is appropriate for his or her pay. Donít forget foreign travel: Is the individual constantly traveling to the same outside continental United States location with no apparent reason to do so?

(4) People frequently ask why we look into a personís background. The following example says it all... A Navy man by the name of Drummon, gave communication secrets to the Soviets. An accounting was made on how much it cost our Government to revamp the electronic devices and rewrite and reissue the codebooks involved. The cost was over $200 million dollars. A current investigation may have identified undue affluence or some other indicator.

(5) A primary aspect of our countermeasures program is to recognize that any member of the US Army, any Government employee or their dependents can become a target of a foreign intelligence approach. Our patriotism, nationalism, or pride is

Figure 2-2. Sample SAEDA briefing (Continued)

the attitude which aggravates and stymies the best of the worldís top intelligence agents. The success of an agent demands that they locate and utilize individuals who will sell their country short. Remember no person, regardless of rank or position, is entitled to classified information without proper need to know.

(6) An agent is just as interested in a private first class or a GS-5 with a copy machine as a colonel or a GS-15 who makes policy. Even if a person does not have a clearance now, a potential target exists. All they want is an employee who is saying, ìI should have been promoted, I should be making more money, maybe with a few thousand dollars I could set things straight or get that BMW.î (If you encounter someone who thinks like this, combined with access to classified information you may have identified a target for espionage.)

(7) To effectively counter espionage you must be aware of the problem, realize that it does exist, and never place yourself in a position which will leave you open to be approached for some type of espionage activity.

(8) Being aware of the security problem and the knowledge of how to react can be compared to the use of a seat belt in an automobile. We would be perfectly happy if it was never put to the use for which it was created, but it is essential when there is trouble. If you are approached, we hope that you will know what to do, and that you will be willing to talk to the right person.

h. Espionage incidents.

(1) In July 1961, Frank Mrkva, a State Department courier, was making routine rounds of the embassies and during a stop at the Czech Embassy, received an invitation to a party to be given by an embassy official. Thus began a 5-year friendship of sorts that ended when the Federal Bureau of Investigation (FBI) revealed that Mrkva had been instrumental in neutralizing a communist intelligence operation. Mrkva had simply reported the first contact with the Czech official, and, under the guidance of the FBI, was able to foil an attempt to place a clandestine listening device in the office of the Under Secretary of State.

(2) In February of 1970, Alexsander V. Tikhomirov was arrested in Seattle, Washington, by FBI agents. At the time, Tikhomirov was working as a translator assigned to the Soviet mission at the United Nations. He had been active in an espionage net that stretched across the United States. It ended when a US serviceman stationed in Seattle reported a meeting with Tikhomirov.

(3) On 17 April 1982, Otto Attilla Gilbert was arrested by FBI agents in Augusta, Georgia. Gilbert, who recently had lived with his mother in Forest Hills, New York, pretended to have fled Hungary after the 1956 uprising. He was actually working for Hungarian military intelligence. His arrest culminated an investigation by US military intelligence and the FBI that started in 1978 in Europe. Gilbert was arrested shortly after he gave $4,000 to Army Chief Warrant Officer Janos M. Szmolka in exchange for classified military documents and microfilm. Szmolka, a Hungarian native, was working in cooperation with the Army counterintelligence and the FBI. Gilbertís arrest was considered to be ìa highly important arrestî because it illustrated ìa penetration operation by an FIS into US military affairs.î

(4) On 28 May 1985, John Anthony Walker and his son, Michael Lance Walker were indicted by a Federal grand jury in Baltimore on six counts of espionage. John A. Walker, a retired Navy warrant officer who had held a TOP SECRET crypto clearance, was charged with having sold classified material to Soviet agents for the past 18 years. During his military career, Walker made some investments in which he lost money. To make up for his losses, in late 1968 at the age of 30, Walker went to the Soviet Embassy in Washington, D.C., and offered his services for purposes of espionage. He compromised key cards used for enciphering messages and also provided information on the encryption devices themselves. At least a million classified messages of the military services and US intelligence agencies were compromised by Walker. A Soviet defector said the KGB considered this the most important operation in its history. Michael L. Walker, a petty officer assigned to the USS Nimitz, was accused of providing classified Navy documents to his father for sale to the Soviets. Fifteen pounds of classified material were in his possession at the time of his arrest on the Nimitz. On 28 October 1987, both John and Michael Walker pleaded guilty to espionage under a plea agreement. On 6 November 1986, John Walker was sentenced to two life terms plus 10 years to be served concurrently. Michael was sentenced to 25 years. John Walkerís arrest was the result of an FBI tip from his former wife.

(5) On 23 August 1988, Clyde Lee Conrad, retired Army sergeant first class, was arrested in West Germany and charged

Figure 2-2. Sample SAEDA briefing (Continued)

with copying and transmitting classified documents to the Hungarian intelligence service for nearly a decade. He was recruited in 1974 by a Hungarian-born immigrant, Zoltan Szabo, a veteran of Vietnam who served as an Army captain in Germany. Szabo began working for Hungarian intelligence in 1967. Two Hungarian-born doctors arrested at the same time in Sweden are said to have acted as couriers in the espionage operation and Conrad is believed to have hired at least a dozen people in the US Army to supply classified information, one of the biggest spy rings since World War II. Conradís recruits continued to work for him after returning to the US, illegally exporting hundreds of thousands of advanced computer chips to the East Bloc through a phony company in Canada. Conrad was granted a TOP SECRET security clearance in 1978 when assigned to the US 8th Infantry Division Headquarters in Bad Kreuznach, Germany. Despite his administrative specialistís job which gave him access to extensive classified materials, Conrad had not been subject to a periodic reinvestigation before his retirement in 1985. Documents provided to Hungarian agents concerned NATOís plans for fighting war against the Warsaw Pact; detailed descriptions of nuclear weapons; and plans for movement of troops, tanks, and aircraft. Conrad, in charge of a vault where all the 8th Infantry Divisionís secret documents were kept, took suitcases stuffed with classified papers out of the base. No one checked on him! The former sergeant is reported to have received more than $1 million for selling secrets. In 1989, Conrad was charged with treason under West German law. It took more than a year to charge him formally due to the complexity of the case which initially was declared one of espionage and then broadened to include the more serious charge of treason. Tried in West German court, Conrad was sentenced to life imprisonment on 6 June 1990.

(6) In all cases, spies have exhibited one or more of these traits:

(a) Excessive indebtedness or recurring financial difficulties.

(b) Homosexual, criminal, or immoral conduct.

(c) Excessive drinking or use of narcotics

(d) Repetitive absence without leave.

(e) Questionable or unauthorized contact with representatives of foreign governments or agencies.

(f) Mental or emotional instability.

i. Remember, under AR 381-12, your reporting responsibilities are:

(1) Report any attempt by an individual to collect classified or sensitive information through documents, observation, or conversation; any attempt by a suspicious acting person to cultivate your friendship; any attempt to blackmail, threaten, or coerce you or your family members.

(2) Finally, if you are in a travel status in a foreign country, report the incident to the nearest US Defense Attache or other Americans in the US Embassy or Consulate. If for any reason you suspect that you have been approached for classified or sensitive information by an intelligence agent, report your suspicions immediately to the Fort Knox 902nd Military Intelligence Resident Office or the USAREC security manager.

(3) Do not take any further action on your own or mention it to anyone to include family, friends, or your chain of command. Remember that family members are also susceptible to FIA approaches. Ensure family members are also aware of reporting procedures.

Figure 2-2. Sample SAEDA briefing (Continued)

a. Security managers must ensure that all personnel are briefed to alert them to their possible exploitation under the following conditions:

(1) Travel to or through special concern countries or other areas of officially announced risk.

(2) Attendance at international scientific, technical, engineering, or other professional meetings in the US or in any other country outside the US where it can be anticipated that representatives of designated countries will participate or be in attendance.

(3) Individuals who travel frequently or attend or host meetings of foreign visitors as described in a above need not be briefed for each occasion, but must receive a thorough briefing at least once every 6 months and a general reminder of security responsibilities before each such activity.

b. These briefings should include those incidents and situations which must be reported. Failure to report the following may be a basis for disciplinary action under the Uniform Code of Military Justice:

(1) Attempts by unauthorized persons to obtain classified or unclassified information concerning US Army facilities, activities, personnel, or material through questioning, elicitation, trickery, bribery, threats, or coercion, either through direct or indirect personal contacts or correspondence.

(2) Attempts by unauthorized persons to obtain classified or unclassified information through photographs, observation, collection of documents or material, or by any other means.

(3) Attempts by persons with known, suspected, or possible foreign intelligence backgrounds, associations, or activities to establish any type of friendship or social or business relationship, or to place Department of the Army (DA) personnel under obligation through special treatment, favors, gifts, money, or other means.

(4) All incidents where DA personnel, or their dependents, traveling to or through foreign areas of special concern, are approached in search of classified or unclassified information.

(5) Nonofficial contacts by DA personnel with persons whom they know or suspect to be members of a foreign intelligence or security service, foreign military or police organizations, or any officials of designated countries.

(6) Official contacts with persons described in (5) above when undue curiosity is shown about a DA member, or when an attempt is made to gain information from the DA member.

(7) Information concerning international terrorist plans and activities posing a direct threat to facilities, activities, personnel, or material.

(8) Known or suspected acts or plots to harm or destroy defense property by sabotage.

c. Immediately report these situations or incidents immediately to the nearest Intelligence and Security Command or tactical military intelligence office. If these are not available, the reports should be made to the unit commander or the unit security manager. Limit dissemination of information regarding the event to as few people as possible and only those who need to know. Reporting procedures are outlined thoroughly in AR 381-12.

d. An example of a foreign travel briefing for personnel traveling to a designated country is contained at figure 2-4 and figure 2-5. Ensure each briefing is tailored to meet the specific situation.

Figure 2-3. Travel briefing (requirements and criteria)

a. This briefing is provided to acquaint you with the risks involved in traveling, primarily in special concern countries, and to furnish guidance to help you cope with those risks.

b. Foreign intelligence services (FIS) use various collection methods when targeting potential contacts. US personnel traveling abroad are considered prime targets of intelligence agents. It is possible that intelligence services are advised well in advance of potential vulnerabilities of American travelers, and that they will take steps to target those persons who can best satisfy their needs. The largest and most active FIS is the Russian SVR (the KGB of the former Soviet Union).

c. Those of other special concern countries are also formidable in size, usually patterned after or run by the SVR (KGB), and usually operate in close collaboration with each other. The two principle objectives of the FIS are: (1) To induce you, willingly or not, to reveal official defense, security, or industrial information on US military, scientific, and technological progress; and (2) To recruit you, through coercion or blackmail, to provide information to them upon your return to the continental United States.

d. In designated countries, visa applications are often checked by agents to determine your immediate or future value to their intelligence requirements. Almost everyone you have contact with while in a designated country, including tourist guides, bell boys, maids, train crews, bartenders and waitresses, and any casual acquaintances you may make, will be questioned concerning your activities. Intelligence agents make extensive use of sophisticated technical surveillance devices. In the main hotels, all telephones can be tapped or used as listening devices even when cradled. TV sets can be used as electronic monitors, and photographic surveillance carried out by instruments not readily detectable by the untrained eye. Two-way mirrors and infrared cameras permit photographs to be taken, even in low level lighting. Bars, cocktail lounges, and restaurants may be fitted with microphones connected to a central monitoring point where conversations can be recorded.

e. Miniature microphones can be inserted in ashtrays, centerpieces, lighting fixtures, etc., and can also be used in cars, trains, buses, and even open air meetings. Tiny radio transmitters with microphones the size of a match head can be hidden in pens, book spines, coat hangers, or even picture hooks on the wall. Eavesdropping by laser beams eliminates the risk of entering a room to plant bugs. The agent can point the laser at a window pane that reacts to the vibrations caused by the sound waves from the conversation conducted inside.

f. Driving regulations in foreign countries, especially in designated countries, are often more complex than those in the US, and are strictly enforced. Any rented car or other vehicle used can be easily traced by electronic monitoring devices. Should you wander off a designated or approved route, you may be subjected to long and perhaps ruthless interrogation.

g. The approach is to compromise and subsequently blackmail a visitor whom they identify as a possible target. Acts which are considered innocuous in this country, or at worst carry a slight moral stigma, are often offenses that are against the law in foreign countries. Designated country intelligence agents are known to entrap visitors in such offenses and then threaten them with arrest and long imprisonment. A variation of those methods of approach are often used as entrapment techniques. You may be invited to take part in some nonofficial financial transaction, such as obtaining local currency for personal use at favorable rates, or selling personal items to a friend or casual acquaintance. These acts violate laws in most foreign countries. You may be approached by a resident and asked to relay a letter, gift, or personal message out of the country to some relative or friend. To take letters or packages either in to or out of a communist country for delivery to private citizens is dangerous and can lead to imprisonment. There is constant risk and danger in taking photographs in designated countries. It is essential that you obtain permission in advance as to ìwhere and whenî a camera can be used.

h. Irregularities in your personal behavior constitute the highest and most productive area of compromise exploitations. Excessive drinking may cause you trouble. You could also be compromised through sexual activity. A liaison visit between you and a local resident would not remain a secret to the intelligence service.

i. The individual may even be associated with the FIS from the outset; if not, that person is likely to be under their control at a very early stage. Homosexual affairs carry the same risks as heterosexual acts, but to a greater degree. Local homosexuals are often deliberately ìbaitedî by agents in front of visitors who are believed to have or exhibit homosexual tendencies. A visitor who commits any offense against local law runs the risk of being arrested or, when faced with photographic or other intimidating evidence, invited, under threat of a withdrawal of your visa, imprisonment, or of public exposure (either to family and friends, or supervisors in the US Government) - to work for them.

j. There are certain precautions you can take to reduce the likelihood of a contact when traveling in a foreign country. When applying for a passport or visa, do not fail to list current or past military affiliation. In one instance, a representative of a tour agency was reported to have advised military personnel to list a civilian occupation in place of their true military status on visa applications on the basis that occasionally visa applications were turned down if a military affiliation was listed.

Figure 2-4. Sample travel briefing (travel to special concern countries)

k. Such evasion of facts would lead to a charge of espionage. Do not make any oral reference to military-related activities. Advise the US Embassy in each country of your complete itinerary. Keep in contact and record the address and telephone number of the nearest US Embassy, consulate, or legation in each city in which a visit is planned. Keep passports on your person at all times and memorize the identification number of your passport. Do not engage in the black-market or other illegal activities.

l. Attempt to learn the laws and rules of the country you are visiting. Be careful about invitations you accept and do not overindulge in drinking or engage in other promiscuous activities. Do not accept letters, personal messages, photographs, packages, or other material to be carried openly or smuggled in (or out) the country, for any reason.

m. Make an extremely accurate and complete declaration of money and valuables on entering designated countries. Retain a copy of the declaration until departure. Never pick up souvenirs, statues, or artifacts, just because they appear to be lying around or unclaimed. Purchase such items in approved shops only, making certain that a receipt is provided for each purchase. Do not sign any receipts for money or service unless a copy is immediately obtainable. Do not make or write any statement which might be exploited for propaganda purposes. Do not sign petitions however innocent they may appear. Do not photograph any military personnel, equipment, installations, defense plants, or other questionable military or restricted areas. Refrain from photographing slum areas, ghettos, or underprivileged persons in the host country. Do not photograph airports and train yards.

n. Be aware that clothing can be tagged with invisible dyes or radioactive materials, either in a cleaning facility or in your room. A letter or some other object placed in your pocket coming in contact with the material could later be traced to you. Use your own stationary and not that furnished by hotels. Purchase stamps at a post office or embassy outlet. Stamps can be tagged with invisible inks or radioactive tracers. Assume that letters will be opened and read. If it is necessary to write about sensitive matters, use Army Post Office channels via the embassy or consulate. Be wary of overly friendly guides, interpreters, servants, etc., who show an undue interest in your welfare. Donít trust them with matters of confidence. Obtain medical or dental services only from US operated or sponsored facilities. In any emergency, contact the US Embassy for advice.

o. If you suspect an approach has been made, or you become involved or entrapped in a conspiracy to commit espionage, you are to report to the nearest US Command, US Embassy Security Office, or Military Attache. If you have been indiscreet or otherwise compromised, you can discuss the situation in confidence with the US security representative. Above all, do not attempt to get out of an embarrassing situation by yourself, or assume the role of self-appointed counterintelligence agent. Immediately report any suspected approach made to you after your travel through your security officer or commander to the appropriate counterintelligence organization.

p. If you are captured or detained, abide by the code of conduct; most countries are signatories of the Geneva Convention and are obligated to treat prisoners humanely. Insist on being allowed to talk to someone from the US Embassy.

q. You are also a prime target for terrorism by any of the terrorist organizations operating in foreign countries. We have learned much from recent terrorist incidents, and two of the most important lessons learned are: The need for personnel to be informed regarding the terrorist threat posed against them. Contact your security manager for terrorist threat information. It is important to react to the threat by implementing appropriate, practical measures, or groups of security measures.

r. Studies confirm that personnel who implement such measures significantly increase their chances of surviving a terrorist threat. Security measures must be practical, imaginative, based on a common sense approach, and tailored to local threat conditions.

s. There are some precautions you must take when traveling, regardless of the mode of transportation. Be aware of the local terrorist threat and have faith in the magnitude of threat assessments made by intelligence and security professionals Recognize the fact that lower ranking and less visible personnel can become targets of terrorist groups when those appearing to be more attractive targets are security conscious and/or well-protected. Be unpredictable. Vary times and routes of travel and modes of transportation to and from work or places of entertainment. Be alert to surroundings and report suspicious

Figure 2-4. Sample travel briefing (travel to special concern countries) (Continued)

behavior and activity to law enforcement and local security or intelligence personnel.

t. Follow the advice of security personnel regarding measures to increase security of your residence or temporary accommodations. Park your car in a protected area if possible and check it for obvious signs of tampering prior to entering and starting the vehicle.

u. In high threat areas, avoid wearing the military uniform in public places and remove headgear when riding in vehicles. Donít flaunt wealth in public. Be cautious in providing information to strangers over the telephone. When in doubt, donít admit strangers to your residence or hotel accommodations without checking their identity with authorities.

v. Keep family members or office personnel advised of your whereabouts and appointments when away from home or office. Become familiar with the area in which you are traveling, to include road networks and locations of unique landmarks such as factories and transportation facilities. Local nationals can often provide an alert to terrorist or extremist actions based on information not available to US authorities or foreign countries.

w. You can enjoy a short trip or extended tour in a foreign country when you are aware of possible threats to your safety. Knowledge of security precautions will help eliminate most vulnerabilities and this briefing should enhance your security awareness. Remember, an ìounce of prevention is worth a pound of cure.î

Figure 2-4. Sample travel briefing (travel to special concern countries) (Continued)

All US Government employees, regardless of position or assignment, are likely to be of interest to intelligence services of designated countries. Special concern country intelligence networks make it their business to learn the identities of Americans, and frequently attempt to target them for intelligence approaches when they travel abroad. The approach may be direct or indirect, highly sophisticated, or crudely obvious. In any case, US personnel traveling to designated countries should be constantly alert to the problems that can befall them. The purpose of this briefing is to make employees aware of the pitfalls associated with such travel, and to advise them on defensive measures against hostile intelligence exploitation.

a. The Bureau of Consular Affairs, US Department of State, frequently publishes advisory material on current travel conditions in designated countries. This material should be available through your agency and you should carefully review any such information covering the country(s) you will be visiting. It is especially important that you are aware of the items which may or may not be taken into these countries.

b. Visa applications are routinely scrutinized by intelligence services of these countries. In order to avoid possible difficulties in this area, it is important that you name any relatives that you intend to visit in the host country.

c. When obtaining visas, travelers should ask the appropriate consular officer how much foreign currency (US and other) and what valuables may be taken in and out of the countries to be visited. Make sure you have enough money for the trip and strictly follow the approved itinerary. You may not import local currency into the countries to be visited.

d. If you are a naturalized American citizen of East European origin, note carefully: There have been instances in which former East European countries have not recognized the US citizenship of former nationals, and have taken the position that such persons retain their original nationality and are therefore subject to treatment as citizens of the country upon reentry into its jurisdiction. If you have a problem for this reason, consult first with the US Department of State for advice and clarification of your status.

e. You may wish to carry with you gifts for friends or relatives. Carry gift items that are neither controversial nor prohibited. Do not bring pornography, narcotics, or political material. Pornography laws in some designated countries are far stricter than those in the US, and you should avoid taking with you magazines or other materials that might be considered pornographic. Any patent medicines or prescription drugs should be clearly for your own use and in reasonable quantities to convince authorities that they are for your personal consumption.

f. Do not carry, on behalf of a third party, any letters, messages, or packages for private individuals in designated countries. You may be deemed guilty of circumventing normal channels of communications, or you may be regarded as a courier for illegal or subversive purposes.

g. Carry only essential forms of identification. Leave Government badges, building passes, etc., at home. Write down your passport number and keep it separate from your passport. Do the same with the address and telephone number of the American Embassy.

h. Do not take this document with you! Study it; think about it; and remember its warnings during your visit. But leave the document at home.

i. Rules governing declarations of valuables and currency and those relating to transactions are strictly enforced. Make an accurate declaration at entry of all money and valuables, including travelers checks. Some countries give the traveler a copy of the declaration, which must be surrendered upon leaving. It is important to keep receipts of all money changes as these are frequently requested upon departure. Undeclared sums of US or other currency is likely to cause difficulty with authorities and may be confiscated upon departure.

(1) You will generally be permitted to take in such items as cameras, transistor radios, etc. It is wise to declare such items as you enter, however, to preclude possible explanations, customs charges, or confiscations when you leave. Baggage inspections may be extremely thorough or only perfunctory. On occasion, your baggage may not even be opened at entry.

(2) As soon as possible after arrival, it is recommended that you contact the American Embassy or Consulate, either by telephone or in person, and provide your local address and the probable length of your visit.

(3) It is unwise for you to drive yourself in a designated country. Try to use public transportation or hire a driver, as local traffic regulations may be confusing. There have been incidents where traffic accidents were deliberately provoked to incriminate or embarrass a visitor.

Figure 2-5. Sample terrorism security briefing (travel in special concern countries)

j. Always assume that your hotel room is equipped with devices to overhear or record your conversations. There may be devices installed through which you can be physically observed, even while your room is in darkness. In addition to the usual microphones, telephones tapes, miniature recording devices, etc., intelligence operatives today use infrared cameras, infrared ìsnooper-scopesî optical lenses, closed circuit TV, and other highly advanced equipment. Do not search for such devices, and do not make an issue of it if you should by chance find one. The presence of such equipment may not necessarily be significant as concerns you. The device may or may not be monitored during your visit, or it may be monitored only on a spot-check basis. Do not try to neutralize such devices by running tap water, playing your radio, etc. Some modern devices are so sophisticated that they cannot be neutralized. Overt efforts on your part to combat such penetration will make you only more suspicious to the intelligence service. The best defense against such devices is the abstinence from other than light, uninformative discussion.

k. Important. Should you discover any device of the above kind, take no overt action against it. Continue your normal conversation giving no indication you have discovered it, and report your findings to the US Embassy, Consulate, or to your security officer upon arrival.

l. Beyond your hotel room, you should assume that conversations in vehicles (including embassy vehicles), train compartments, restaurants, conference rooms, and other public places may be monitored. Miniature microphones with transmitters or recorders can easily be secreted on the person or an individual in your group. It is even technically possible to record your conversations in open, outdoor areas; however, those areas are normally more secure than indoor locations.

m. Avoid unnecessary discussions concerning your job, your workplace, and other official matters. Also avoid discussing other US employees habits, character, or other matters which reveal weaknesses or idiosyncrasies.

n. Assume that your personal luggage will be searched at some time in your hotel room. If you discover evidence of this, do not make a big issue of it. Report positive evidence of such activity to the US Embassy and to your security officer upon your return. It is just as well not to bother locking your luggage, as most locks are readily picked. This will only increase the curiosity of the intelligence agent and the lock may be broken. Never leave your luggage unattended containing valuable papers or documents you do not want anyone else to read. If you surprise someone searching your possessions, donít take any violent or physical action, but report the incident to local and US authorities.

o. You may receive a ìwrong numberî or other mysterious telephone calls in the hotel room at any hour of the day or in the middle of the night. Do not let this unduly upset you. It may be a crude but effective method of determining whether or not you are in your room. It may be only a result of poor telephone service.

p. Do not rely on hotel employees for protection service. In these countries, you should assume that chambermaids, elevator operators, and hotel employees, as well as the waiters or the waitresses in restaurants, are in the employ of the intelligence services. Be particularly circumspect in your relations with guides, interpreters, and designated country travel agency personnel as these people are invariably used by intelligence agencies.

q. You may be placed under physical surveillance as you travel either on foot or by vehicle. You may suspect you are being observed when actually you are not. In either event, it is best to ignore it. Intelligence agents at various times observe visitors on a spot-check basis for no apparent reason. On the other hand, they may be collecting detailed data concerning your activities in preparation for a more direct intelligence approach. Do not attempt to lose the surveillance. If you are actually being followed for intelligence objectives, you will be covered by a team of several agents, and your evasion attempts will make you more suspicious.

r. You will be permitted to take photographs with your personal camera, but be careful not to photograph restricted areas. Travelers should refrain from taking photographs from aircraft, photographing military and police installations and personnel, industrial structures, harbor, rail and airport facilities, and border areas. Designated countries also resent you photographing items which put them in a bad light, such as slum areas, public drunks, scenes of civil disorder, or other public disturbances. If you do take such photographs, your film may be confiscated.

Figure 2-5. Sample terrorism security briefing (travel in special concern countries) (Continued)

s. Be particularly circumspect in approaches which may be made offering social companionship, especially of a sexual nature. Many of these persons are ìplantsî of designated country intelligence agencies and will offer themselves attractively for the purpose of getting you in a compromising situation which will be followed by blackmail threat to force your cooperation in intelligence activities. Under no circumstances should you seek or accept this kind of social companionship in a Communist country. The intelligence services are fully aware of the possibilities inherent in human frailties, and will capitalize immediately upon any indication of immoral or indiscreet behavior of American travelers. Even when failing to detect a vulnerability, agents have attempted entrapment of innocent travelers.

t. For this reason, you should maintain the highest level of personal behavior at all times, avoid long walks at night alone, and endeavor to always be in the company of someone you can trust. Be especially careful to stay well within your capacity for alcohol so as not to weaken your defense or lose your self-control.

u. Do not accept from anyone (including friends, relatives, or professional contacts) letters, photographs, packages, or any other material to be smuggled out of the country or carried in your effects when you depart. Be firm in your denials in these matters, as such requests may be acts of intelligence provocation to entrap you.

v. Bear in mind that there are many political, cultural, and legal differences between the US and special concern countries. Actions which are innocent or, at worst, carry wrist-slapping penalties in the US, are often considered serious offenses in other societies. Persons violating the law, even unknowingly, run the risk of arrest or expulsion. Do not, for instance, take souvenirs from hotels or institutions, however insignificant in value they may appear.

w. Do not engage in any private currency transactions with individual citizens. Do not try to sell or trade any personal item, including clothing, which you have brought into the country, or purchase bargains from street peddlers or questionable vendors. Do not engage in black market activities. Many designated countries have laws governing exportation of art work and historic relics. Be familiar with these laws if you intend to purchase such items, and make these purchases only at official establishments.

x. Should you be detained or arrested for any reason by police or other officials of these countries, be cooperative, but insist promptly, politely, and repeatedly, if necessary, that the US Embassy or Consulate be notified. Do not make any statements or sign any documents you do not fully understand until you have had an opportunity to confer with an embassy representative. You may possibly be accused of having some connection with an American intelligence service, or of having accepted an assignment by such service to be carried out in the host country. You should make no admission whatever indicating you have even had any dealings, under any circumstances, with any US intelligence agency.

y. Mail which you receive or transmit is subject to censorship in a designated country. In all mail you write prior to, during, or after your visit to a designated country, make no reference to classified information nor reveal information of possible value to their intelligence services. Be careful in writing to or about relatives or friends in these countries, as they may become targets for investigation or exploitation.

z. There have been several incidents in designated countries wherein speech inducing drugs, medicines, etc., have been used for the purpose of aiding in interrogation. In nonemergency situations, make every effort to avoid hospitals or medical facilities without first having notified the US Embassy or Consulate.

aa. Immediately report any action which might form the basis of pressure or compromise, or any attempt to pressure or compromise you, to the American Embassy (security officer) in the country being visited, and also to your security manager immediately upon your return to your job. Also report any unusual subsequent contacts with country nationals.

ab. We have discussed many, but not necessarily all pitfalls which may befall an American traveler. New espionage techniques and tactics are constantly being developed, and the highest degree of alertness is necessary at all times. While the techniques employed by designated countriesí intelligence services seem farfetched, illicit, or taken from ìspy novels,î they are in fact used in day-to-day activities and operations. Although these techniques are revolting to an American, one must nevertheless recognize them as a part of their system in order that he or she may successfully counter such practices.

ac. Well, so much for the dark side of the picture. All of these things had to be said so you could be forewarned of the

Figure 2-5. Sample terrorism security briefing (travel in special concern countries) (Continued)

possibilities. Now for the probabilities: You probably will not be entrapped by an intelligence agent, and you probably will not have any problems if you respect local laws and customs, be honest in your dealings and behave discreetly. You can expect friendly treatment from most of the citizens with whom you come in contact and you will find that they are very interested in all aspects of American life. You can therefore serve as a valuable good will ambassador for the US while you enjoy the interesting and innocent features of the country(s) you visit. Be open to this experience, have a good trip, and come home safely.

Figure 2-5. Sample terrorism security briefing (travel in special concern countries) (Continued)

No nation or individual is immune from acts of terrorism prompted by political extremism. The likelihood of terrorist incidents varies from country to country and depends, at least in part, upon the stability of the local government and the degree of frustration of terrorist groups or individuals. However, there is currently a disturbing trend for terrorist attacks to be carried out in neutral nations where terrorists have no apparent interests. The point is, terrorism can occur in the least likely location.

a. In many instances US military personnel and facilities have been the object of terrorist attacks. While there is no absolute protection against terrorism, there are a number of reasonable precautions that can provide some degree of individual security. The objective of employing personal security measures in your daily life is to make you alert to terrorist attacks, help eliminate predictable patterns of activity, and basically for you to keep a low profile. This will make you a less likely target.

(1) Personal security precautions. Attacks and kidnappings of US personnel abroad have taken many forms. The most common kidnapping tactics used to date have been to intercept individuals in their automobiles. These attacks have several common features such as: Two vehicles were used by the kidnappers, they had approached from the center of the roadway, and three or more attackers were involved. By using safe driving techniques and adequate personal travel precautions, the possibility of successful vehicular attacks and kidnappings can be substantially reduced.

(2) To the extent possible, avoid establishing a pattern in the routes and times of your movements to and from work, shopping, and around town. Past kidnappings indicate that kidnappers generally keep victims under surveillance for substantial periods of time (several days to several months) to discover travel patterns and arrange a suitable time and place for the kidnapping. Unpredictability is one of your best weapons.

(3) When going out for any reason, avoid going alone. Try to travel with a group of people; there is safety in numbers.

(4) If possible, travel in a convoy, particularly while traveling long distances.

(5) Avoid isolated back-country roads and areas of the city which are known to be dangerous. On multiple-lane highways, drive toward the center of the road to make it more difficult for your car to be forced to the curb.

(6) When traveling in a car, keep all doors locked. Keep windows closed, or opened only a crack. Avoid types of cars or actions that might identify you as an American or as someone rich or important.

(7) Park cars off the streets at night. Lock cars, no matter how short a time they may be unattended. If it is necessary to leave car keys with a parking attendant, leave only the ignition key.

(8) Before entering your car, ascertain that there are no suspicious objects or unexplained wires or strings inside or underneath. Never attempt to remove a strange device or object yourself. Contact the local police or US officials if you find a possible explosive device on your car.

(9) Be sensitive to the possibility of surveillance. Before leaving your home or office, check street for suspicious cars or individuals before departing. Try to have a police security check or background check on all local employees, such as domestic help.

(10) Your office and home should have a record of any medical problems that may be expected in an emergency. Information should include ailment, type of medicine, doctorís name and address, blood type, allergies, etc.

(11) Vehicle preparations. You never know when you might have to take evasive maneuvers with your car. Keep it in top working condition.

(12) Sirens and antidisturbance devices (alarms) may be fitted to your vehicle.

(13) Keep vehicle maintenance up-to-date. Never allow the gas tank to drop below half-full to avoid running out of

Figure 2-6. Sample terrorism security briefing

gas enroute somewhere or in tight situations. Equip vehicles with hood and gas cap locks to prevent tampering or the concealment of explosives.

(14) Install side view mirrors, right and left. Do not overload, keep a clear field of vision to the rear and know your vehicle and its capabilities.

(15) Emphasis should be placed on using young, agile types, preferably with a police background for a chauffeur. Thoroughly brief the individual on tactics for use in an emergency situation and to never leave the vehicle during a public function.

(16) Evasive actions. Most terrorist attacks have taken place in areas where there are side streets, this can work to your advantage. If you have an indication that you are being followed, take evasive action immediately.

(17) Make a relatively high speed turn in either direction and circle the block.

(18) If following continues, seek a safe haven such as a police station. If equipped with radio, inform stations monitoring, request help.

(19) In the event of a fire-fight between local authorities and terrorists, get down and stay down. Unless you are in the direct line of fire, it is suggested that you do not move. Experience has shown that often times anything that moves gets shot.

(20) In taking evasive action, if it becomes necessary to jump a curb, median strip, or traffic island, it must be done with care to avoid disabling your vehicle.

(21) If possible, put another vehicle between yourself and pursuers.

(22) Constantly observe to note whether you are being followed to or from work or other places you frequent; if so, notify police promptly.

(23) Be alert at all times when traveling in a car. Do not depend on anyone elseís senses, especially a foreign national driver. If someone does appear to be following you, try to get the license number and lose them quickly. The best tactic is to drive immediately to a police station.

(24) When driving, keep a good distance between you and the vehicle in front of you; especially a truck. Should this vehicle stop suddenly, you will have additional time to avoid it and not be boxed in.

(25) Avoid hitchhikers and do not stop to see any commotions that may be taking place on the street; this may be the distraction for an ambush.

(26) If driving and signaled to pull over by a police car clearly marked as such, or if you encounter a road block manned by uniformed police or military personnel, you should stop and remain seated inside your car. If asked for identification, roll the window down enough to pass your identification to the officer. Do not unlock the doors.

(27) Avoid using any one taxi or bus stand regularly. Vary your choice between first, second, and third on a random basis. Such action can help avoid a ìplant.î Whenever possible do not use taxis.

(28) Be aware when phoning for a taxi to pick you up at home or office that your phone may be tapped and you could get a ìterrorist taxi.î

(29) Do not allow a taxi driver to deviate from a desired route. Ensure children are accompanied when traveling by taxi.

(30) Security measures for the office. Do not stand or place desk directly in front of windows.

Figure 2-6. Sample terrorism security briefing (Continued)

(31) Avoid routine trips to the office during hours when no one else is there.

(32) Be alert to anyone loitering near the office.

(33) Come and go at different times and use varying routes and entrances to the building, when possible.

(34) Establish a package control area for incoming mail and parcels; this should be a room away from work areas.

(35) Suggested behavior in case of kidnapping although it is recognized that hard-and-fast rules cannot be applied in kidnappings, the following points are worthy of special consideration.

(36) If it is impossible to evade the kidnappers and they get close enough to fire directly at the driver, surrender immediately. Do not attempt to flee on foot. A US Ambassador in Guatemala was shot and killed attempting to escape by running away. In general, you may attempt evasion as long as you are in a moving car in no immediate danger of being shot. Do not attempt to physically struggle with your kidnappers; a US official in Argentina was shot several times while trying to fight off terrorists. Remember, these people are under pressure and are unpredictable.

(37) Under all circumstances attempt to stay calm and be alert to situations that you can exploit to your advantage. Remember, the primary objective of family and law enforcement officials is to secure your safe return as quickly as possible. No matter how ìreasonableî your captors may appear on the surface, they cannot be trusted to behave normally and their actions may be unpredictable.

(38) Comply with instructions of your abductors as well as you can. Do not discuss what action may be taken by your family, friends, or company.

(39) Make a mental note of all movements including times in transit, direction, distances, speeds, landmarks along the way, special odors, and distinctive sounds like bells, construction, voices, etc.

(40) Whenever possible, take mental notes of the characteristics of your abductors, their habits, speech mannerisms, and what contacts they make.

(41) Avoid making provocative remarks to your abductors. As noted, they may be unstable individuals who react irrationally.

(42) Immediately request special medicines or medical attention if you have a disease or physical condition which requires treatment.

(43) Try to establish some kind of rapport with your captors.

(44) Before attempting to escape, calculate the chances of success very carefully. Remember, these people have spent weeks and possibly months planning this operation. Are you well prepared?

(45) Security measures for home and family. Identify the best housing available. An apartment house offers the benefit of close neighbors but also offers semipublic access to the lobby and service areas, which is a disadvantage. If a separate dwelling is selected, attempt to locate one with high walls around it.

(46) Make your residence as burglar proof as possible by installing a burglar alarm system and using exterior lighting or even an exterior floodlight system activated by intrusion-detection devices. Other safeguards include deadbolt locks on doors; key locks; iron grilles or heavy screen for ground-floor windows; care in securing upper story windows accessible by trees, low roofs, balconies, etc.; and unusual doors such as sliding glass or French.

(47) Instruct members of the household not to admit strangers without proper identification. A peephole or small window aperture in a door where visitors can be observed prior to entry is recommended. Never leave garage doors unlocked. An uncalled plumber, electrician, or garbage collector could be a disguise to gain entry.

Figure 2-6. Sample terrorism security briefing (Continued)

(48) Consider having a watchdog inside or outside your house, or both.

(49) Have a security or background check of all servants. A servant who is trustworthy may also be a political activist.

(50) If local police protection is available and appears needed, request a patrol through your neighborhood as frequently as possible. Where police patrols are infrequent or nonexistent, employ a private security patrol, perhaps in cooperation with neighbors.

(51) Arrange to have your children escorted to and from school. Instruct school authorities that under no circumstances are they to be picked up by persons other than family members or specifically authorized people.

(52) Do not permit unaccompanied children to use taxis and public transportation.

(53) Do not discuss sensitive information, such as detailed travel plans; or business dealings within hearing of servants. Instruct household members about their security responsibilities.

(54) Treat suspicious letters and packages with care. Examine mail for the following features: Excessive weight for size, springiness in the top, bottom, or sides, protruding wires or strings, the odor of almonds, uneven balance, envelope stiffened with cardboard or other material which may contain a spring-loaded striker, a letter containing another envelope addressed personally to a high official, an inner letter tied with string, a letter with a grease spot. Only an expert should open suspected packages and letters. The best procedure is to isolate them until an expert can be contacted. Do not put them in a bucket of water, since this may make the paper soggy and cause spring-loaded devices to detonate.

(55) Maintain a current list of emergency telephone numbers, and make sure that it is easily available at all times.

(56) Recognize that potential kidnappers may possibly tap your telephone. Be most discreet on the telephone in discussing information concerning travel.

(57) Do not hand out business or home telephone numbers indiscriminately.

(58) Be alert to persons disguised as public utility crew members, road repair workers, etc., who might station themselves near your house to observe your activities. (In one case, a kidnapper disguised as a fruit peddler set up a fruit stand near the victimís house.) Report such incidents to the police for investigation.

(59) Locate a neighborís or public telephone near your home and advise your servants and family of its location for emergency use. Maintain friendly relationships with your neighbors.

(60) Do not become involved in disputes with local citizens. If others initiate troublesome incidents, leave the scene as quickly as possible.

(61) Establish a room or area in your home as a safe haven, a place for you and members of your family to go that is safe in case of a break in or a civil disturbance. Preferably select a room without windows and with a secure door to be a shelter to wait out any intruders until help arrives.

(62) Make up an emergency kit for your home which at least includes: Fire extinguishers (water and CO2), emergency supply of fresh water, a 5-day supply of canned food, candles, blankets, two flashlights and extra batteries, a sterno stove and adequate fuel, an axe, first aid kit, and any special items dictated by the local government.

(63) These checklists are guides. They will assist you in your security if you utilize them properly.

b. The possibility that US military personnel stationed abroad will confront a terrorist act is statistically slight. The problem is nonetheless significant due to the nature and danger of such confrontations. While there is no sure way to

Figure 2-6. Sample terrorism security briefing (Continued)

prevent the occurrence of an act of terrorism, there are precautions which will minimize the threat to the military member and his or her family.

c. Knowledge of these measures and adherence to a few basic security principles will increase the familyís security. Such knowledge should also improve the familyís morale by lessening an element of uncertainty inherent in the overseas tour. If, in fact, the US military family attains a more positive perspective on their assignment, the military member will probably do a better job. A man who is constantly concerned that he and his family are in danger can hardly be expected to mix easily with his host government counterparts.

d. In the past 5 years terrorism has increased alarmingly. There is no evidence that it will cease to be a problem in the future. Some of these measures may appear excessive or ìconspiratorialî to people accustomed to life in the US; however, a cautious approach to sharing information with others and the extra effort to avoid a routine could be the difference between being targeted and not being targeted by terrorists.

Figure 2-6. Sample terrorism security briefing (Continued)

Questions frequently arise regarding the interpretation of AR 381-10 terms like ìcollection,î ìUnited States person,î and ìquestionable activity.î The following definitions and answers are taken directly from AR 381-10.

a. Collection. Information shall be considered as ìcollectedî only when it has been received for use by an employee of a DOD intelligence component in the course of his official duties. For information to be ìreceived for useî and therefore ìcollectedî by an Army intelligence component, an employee must take some affirmative action that demonstrates an intent to use or retain the information received (such as production of a report, filing of an investigative summary, or electronic storage of received data). Establishment of ìunofficial filesî and the like may not be used to avoid the application of this procedure (procedure 2).

b. The term ìUnited States personî means:

(1) A United States citizen;

(2) An alien known by the DOD intelligence component concerned to be a permanent resident alien;

(3) An unincorporated association substantially composed of United States citizens or permanent resident aliens;

(4) A corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments (AR 381-10).

c. ìQuestionable activity.î Refers to any conduct that constitutes, or is related to, an intelligence activity that may violate the law, any Executive Order or Presidential directive, including E.O. 12333, reference (a), or applicable DOD policy, including this regulation (procedure 15).

d. ??????????????????????????????????QUESTIONS??

(1) Can information on US citizens be collected? ìInformation may be gathered by intelligence components using techniques described in procedures 5 through 10 for other than foreign intelligence or counterintelligence (CI) purposes. However, such collection must comply with the following: be based on a proper function assigned to the intelligence component; employ the least intrusive lawful investigative technique reasonably available; and comply with the appropriate provisions of this regulationî (procedure 1).

(2) What is the first step in determining whether an intelligence component may conduct an investigation that involves a US person? ì. . . . the component should first determine whether it has the mission and authority to conduct the type of investigation involvedî (procedure 1).

(3) Who can grant approval to conduct any activity authorized by AR 381-10? ìRequests to conduct any activity authorized by this regulation that requires HQDA or higher level approval (such as the Secretary of the Army or the US Attorney General) will be submitted through command channels to HQDA (DAMI-CIC), WASH DC 20310. Complete justification must accompany each requestî (procedure 1).

(4) Must you report a ìquestionable activity?î ìEach employee shall report any questionable activities to the General Counsel or Inspector General for the DOD intelligence component concernedî (procedure 15).

Figure 2-7. Explanation of terms (US Army Intelligence activities information)

1. AR 381-10 applies to all personnel assigned to USAREC. This regulation is a broad document which covers all US Army intelligence activities to include those directed against both US and non-US persons.

2. The regulation is organized into fifteen procedures. Following is a list of the procedures and their general content:

a. Procedure One, General Provisions, Applicability and Scope Prohibition Against Special Activities and Assassination.

b. Procedure Two, Collection of Information about US Persons.

c. Procedure Three, Retention of Information about US Persons.

d. Procedure Four, Dissemination of Information about US Persons.

e. Procedure Five, Electronic Surveillance.

f. Procedure Six, Concealed Monitoring.

g. Procedure Seven, Physical Searches.

h. Procedure Eight, Searches and Examination of Mail.

i. Procedure Nine, Physical Surveillance.

j. Procedure Ten, Undisclosed Participation in Organizations.

k. Procedure Eleven, Contracting for Goods and Services.

l. Procedure Twelve, Provision of Assistance to Law Enforcement Authorities.

m. Procedure Thirteen, Experimentation on Human Subjects for Intelligence Purposes.

n. Procedure Fourteen, Employee Conduct.

o. Procedure Fifteen, Identifying, Investigating, and Reporting Questionable Activities.

3. AR 381-10 does not serve as the authority for you or any member of any intelligence activity to engage in the above listed procedures. It simply provides guidelines for the conduct of such activities if your unit or staff section has a legitimate mission tasking. Contact the Director of Security before you attempt to engage in any procedure relating to AR 381-10.

Figure 2-8. Information paper (US Army Intelligence activities procedures)

US Army Intelligence Activities Synopsis

Reference: AR 381-10, US Army Intelligence Activities.

This synopsis of the regulation outlines the procedures, restrictions, and requirements for the collection of information by intelligence activities regarding US persons.

1. AR 381-10 does not serve as the authority for any intelligence mission or function, but rather is the standard regulating mechanism for such mission and functions. It pertains to all US Army Intelligence activities, to include those directed against non-US persons. It applies to intelligence units that support unified or specific commands, intelligence staff offices supporting military commanders at all echelons, and other Department of the Army military personnel and civilian employees when they engage in authorized intelligence activities.

2. Summary of procedures 1 through 4 and 14 and 15.

a. Procedure 1, General Provisions. Explains the purpose of AR 381-10 and what the regulation does and does not prescribe. It mandates that the collection of any information by Army Intelligence must:

(1) Not infringe on the constitutional rights of any US person.

(2) Protect the rights of privacy for all persons.

(3) Be based on assigned functions.

(4) Employ the least intrusive lawful technique(s).

(5) Comply with all regulatory requirements.

Procedure 1 also states that Army Intelligence activities are prohibited from conducting or providing support to ìSpecial Activitiesî except in time of war or by Presidential approval and directed by the Secretary of Defense. In addition, the following applies:

(6) Under no circumstances will Department of the Army employees engage in, or conspire to engage in assassination.

(7) All questions of interpretation and/or requests for exception to policy will be referred to the Directorate of Security or the Inspector General.

b. Procedure 2, Collection of Information About US Persons. Information which identifies a US person may be collected by an Army Intelligence component only if the information is necessary to the conduct of a function assigned to the component and provided the information falls in one of the following 13 categories:

(1) Category 1, information obtained with consent.

(2) Category 2, publicly available information.

(3) Category 3, foreign intelligence (includes international terrorism).

(4) Category 4, counterintelligence.

(5) Category 5, potential sources of assistance to intelligence activities.

(6) Category 6, protection of intelligence sources and methods.

Figure 2-9. Briefing format

(7) Category 7, physical security.

(8) Category 8, personnel security.

(9) Category 9, communications security.

(10) Category 10, narcotics.

(11) Category 11, threats to safety.

(12) Category 12, overhead reconnaissance.

(13) Category 13, administrative purposes.

Remember: As soon as nonessential information is filed or incorporated into other material, or some other act is taken to use or retain the information, a reportable violation has occurred.

c. Procedure 3, Retention of Information About US Persons. Essential information acquired under Procedure 2 is authorized for retention and is governed by AR 25-400-2 or other specific records management regulations for unique functions. Retained information must be reviewed annually. Information obtained ìby chanceî can only be retained if it is information that could have been collected intentionally under Procedure 2, provided it falls into one of the following categories:

(1) The information must be necessary to understand or assess foreign intelligence or counterintelligence.

(2) The information must be either foreign intelligence or counterintelligence which has been collected from electronic surveillance.

(3) The information must be incidental to other authorized collection and indicate some involvement in activities that may violate federal, state, local, or foreign law.

d. Procedure 4, Dissemination of Information About US Persons. The dissemination of information about US persons, without their consent, can occur only: (1) When the determination has been made that prospective recipient will use the information for a lawful Government function; and (2) That the information is needed by that prospective recipient for that particular function; (3) If it fits completely into one of the five categories outlined in Procedure 4. Any dissemination beyond the limits outlined in Procedure 4 must be submitted through command channels and approved in advance by HQDA (DAMI-CI) WASH DC 20310.

e. Procedure 14, Employee Conduct. Individual employees will conduct intelligence activity only as prescribed by AR 381-10, and in conducting such activities, will not exceed the limits of the law.

f. Procedure 15, Identifying, Investigating, and Reporting Questionable Activities. Employees will read and become familiar with AR 381-10 and will report any ìquestionableî intelligence activities or violations immediately to the USAREC security manager or unit or directorate security manager.

****

Briefing Acknowledgment

I am familiar with, have read, understand, and will comply with the provisions of the regulations.

NAME DATE

SIGNATURE

Figure 2-9. Briefing format (Continued)

Chapter 3
Inspections and Assistance Visits

3-1. Inspections

a. An effective inspection program ensures compliance with established procedures and regulations, identifies security weaknesses, and recommends corrective action where required. All Headquarters, United States Army Recruiting Command (HQ USAREC) directorates, the United States Army Recruiting Support Brigade (RS Bde), and recruiting brigades (Rctg Bdes) are subject to annual security inspections.

b. SMs at each level of command and staff must conduct inspections and spot checks of their own activities as well as inspect subordinate SMs. Conduct inspections in accordance with procedures prescribed below.

3-2. Annual, announced security manager inspection

a. SMs must conduct an annual, announced security manager inspection (AASMI) each calendar year.

b. Review unit security SOPs, previous inspection reports, spot checks, and records of advice and assistance visits to identify previous security findings and weaknesses.

c. Determine the scope and depth of the inspection, the size of the element, classified document holdings, and number of personnel who work with classified information and the mission.

d. Inspection checklists, if used, should only be used as a guide to conduct the inspection. The scope of the inspection is not limited to the content of a published checklist. A determination of which areas to be inspected must be accomplished prior to the inspection. Review appropriate regulations as needed.

e. Schedule the inspection with the unit or section being inspected.

f. Conduct the security inspection, make on-the-spot corrections when time permits. Outbrief the activity supervisor and/or SM on deficiencies noted during the inspection.

g. Make a written inspection report with findings, recommendations, and comments using format at figure 3-1.

h. Maintain a copy of the inspection report and provide copies of the report to the commander or director of the inspected unit or activity. Units or sections that conduct self-inspections must maintain a copy of the report and forward a copy of the report to the next higher headquarters. SMs at all levels must maintain inspection reports which are reviewed during the annual command security or inspector general inspection.

i. Brief the commander of the unit or section inspected on all findings and shortcomings noted during the inspection and recommend corrective action.

j. Inspected units or sections should be given 30 days to correct findings. A written endorsement of what was done to correct the findings must be submitted to the SM.

k. Units and activities that receive an inadequate inspection rating are to be reinspected within 180 days. Reinspect or conduct an advice and assistance visit to ensure findings have been corrected.

3-3. Unannounced after duty hours inspection

SMs must conduct semiannual unannounced after duty hours inspections (UADHI). The responsibility for conducting these inspections is the same as described in paragraph 3-1. Conduct UADHI using the following guidelines:

a. Review unit security SOPs, previous inspection reports, and note any repetitive findings.

b. Make arrangements to gain access to work areas.

c. Conduct the inspection.

d. Outbrief the SM or staff duty officer (SDO) on any deficiencies noted during the inspection.

e. Maintain a copy of the inspection report. Reports are subject to inspection during the annual security or inspector general inspection.

f. Discuss findings with section leaders where deficiencies are noted. Brief the commander when serious deficiencies warrant command attention.

3-4. Spot checks

SMs who are responsible for conducting AASMI must also conduct quarterly security spot checks. SMs must use their own discretion on the scope of the spot check and what areas require inspecting. As a minimum, SMs should check routine procedures used by personnel who handle classified material during their daily operation. Correct procedural violations of security SOPs on the spot when possible. Maintain record of spot checks conducted in SMís files.

3-5. Advice and assistance visits

SMs are required to make themselves available to subordinate SMs to answer questions and provide assistance on security matters. These visits can be either scheduled or requested. The inspector records the visit on a memorandum for record. Maintain this memorandum for record until the next visit to the same element. These visits are solely for the benefit of the subordinate SM.

3-6. Security rosters

The SMs must maintain a roster of all assigned individuals. Record briefings and debriefings and all security training to include SAEDA training. Maintain this information for 60 days after the individual has departed the section or unit.

3-7. Recordkeeping

a. SMs must keep complete written records of all actions related to security. SMs should maintain these records in one single area for easy access. Records include, but are not limited to, SAEDA training, AASMI, UADHI, arms and ammunitions (A&A) visits, courtesy inspections, annual files inspections, AR 381-10 briefings, certifications for reproduction machines, restricted areas, and open storage areas, security clearance actions, orders of SM appointment, security reference material, etc.

b. Maintain all records in accordance with AR 25-400-2.

REPORT OF SECURITY MANAGER INSPECTION
OF
(UNIT AND LOCATION)

SECTION I. INTRODUCTION

1. On (date) an (announced) (unannounced) security inspection was conducted of (activity) by:

List representatives by title, first name, middle initial, and last name.

2. The following representatives accompanied the security inspection team:

List personnel by name, rank, and position.

3. The last security inspection was conducted on (date).

SECTION II. SCOPE

4. The inspection included the following (elements, offices, sections) of (unit). This paragraph should not be used to indicate a general resume of what aspects of the program were inspected.

SECTION III. FINDINGS AND RECOMMENDATIONS

5. Uncorrected or repeated findings from previous Report of Security Manager Inspection: Indicate ìNONEî if there are no uncorrected or repeated findings.

6. Current findings: Use this paragraph to record findings resulting from this inspection and following together with appropriate recommendations. If there are no findings, indicate ìNONE.î

a. Findings:
Recommendations:

b. Findings:
Recommendations:

7. Only those aspects of physical security relating to classified storage were inspected.

SECTION IV. COMMENTS

8. Comments:

a. Security Education Program: (Evaluate according to requirements of AR 380-5 and AR 381-12. Comment on the general knowledge of assigned personnel.)

b. Lock Modification: (Check all security containers for modifications.) Note changes which would compromise the security integrity of the equipment.

c. Reproduction of Classified Information: Inspect the area, the equipment, the SOP, and access control, warning notices, and any authorizations pertinent to the reproduction.

SECTION V. EXIT BRIEFING

9. All findings and recommendations were discussed during an exit briefing on (date) for the following unit representatives:

List according to rank, title, first name, middle initial, last name, and position.

SIGNATURE BLOCK

Figure 3-1. Sample security inspection report format

Chapter 4
Protection and Storage of Classified Material

NOTE: It is the responsibility of all users and holders of classified information to safeguard it and to limit access on the basis of a proper security clearance and the need to know. The SM is responsible for ensuring that all handlers of classified material are aware of and comply with this requirement. He or she must also ensure that adequate measures are taken to safeguard the material while it is in storage. These are custodial responsibilities. The custodian of classified material is the person who has it in his or her possession. (AR 380-5.)

4-1. Security containers

Only General Services Administration (GSA) approved security containers are authorized to store classified material. Security containers are required to have a GSA-approved label. (For exception to this policy see para 4-4.) Mark each container externally with a number or symbol (AR 380-5) which identifies the safe number. This marking is for identification. It cannot, however, indicate either the level of classified material contained within the container or the evacuation priority.

4-2. Forms

Complete an SF 700 (Security Container Information) for each container (fig 4-1). Each container requires an SF 702 (Security Container Check Sheet) posted (fig 4-2). Use reversible open and closed signs for each container. Post an emergency evacuation and destruction plan in each office having a security container(s) (AR 380-5).

a. SF 700. Complete SF 700 and place part 1 on the inside of the containerís lock drawer. Mark parts 2 and 2A with the highest overall classification of the material stored within the container. Complete part 2A, which identifies the combination, detach and insert into part 2 (envelope). Seal part 2 envelope and store in the master container. Account for SF 700 marked TOP SECRET (TS) in the same manner as other TS documents. Record and maintain names of additional personnel who have knowledge of the combination inside the front of the control drawer of each security container (AR 380-5).

b. SF 702. Display SF 702 conspicuously on each security container storing classified material. It must reflect an entry for each normal duty day and nonduty day the container is utilized. In addition, record the date and time of each unlocking and locking of the security container. The final locking of the day must also show the initials and time the container is double-checked. Someone other than the person locking the container must perform this task. Any available individual may conduct the double-check. If a container is not opened on a normal duty day, record the date, followed by ìNOT OPENED,î initials, and time container was checked. The SF 702 must be kept on file for 24 hours after it has been filled out on both sides, then destroyed, unless it is needed for an investigation of a possible security infraction or violation (AR 380-5).

4-3. Combinations

a. Change combinations to security containers at least annually, or when a person having access to the container is transferred, discharged, reassigned, or his or her security clearance is revoked or suspended.

b. Also change combinations if the combination has been compromised, or the container was found unlocked and unattended (AR 380-5).

c. When North Atlantic Treaty Organization (NATO) information is stored in the container, change the combination every 6 months. (AR 380-5.)

NOTE: Combinations to security containers holding classified material are classified and must be handled and stored accordingly. It is the individualís responsibility to memorize the combination. The combination cannot be kept in a purse or wallet, written on a desk calendar, or kept within the confines on someoneís desk.

4-4. Certifications

All security containers must display a GSA-approved label. If the GSA label is missing, the container must be examined by the SM or a certified locksmith to ensure it meets GSA standards. A memorandum identifying the inspector and date of the inspection must be maintained at the front of the locking door. GSA-approved field safes and one-drawer security containers may be used to store classified information if they are secured to a solid, permanent fixture by a chain and padlock.

4-5. Open storage

There are no areas within the United States Army Recruiting Command (USAREC) authorized for the open storage of classified materials. Requests for open storage of classified material (SECRET or CONFIDENTIAL) must be approved by ~~Headquarters, United States Army Recruiting Support Brigade (HQ RS Bde),~~ the USAREC Security Office ~~Division~~. Forward request for approval to the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ with complete description of area to be used and a comprehensive justification. Convenience is not considered ample justification.

4-6. Container markings

While each container must be marked externally with a number or symbol, no container shall be marked externally to indicate the level of classification of material contained, evacuation priority, nor will it show that a drawer contains only classified waste material. Record the containerís number or symbol on SF 700, part 1. Place evacuation priority markings on each drawer in such a manner that it is visible only when the drawer is open, and not visible when the drawer is closed. (AR 380-5.)

4-7. Custodian precautions

Care during duty hours.

a. Cover sheets. Keep classified material removed from storage under constant surveillance and covered when not in use. Attach cover sheets: SF 705 (CONFIDENTIAL Cover Sheet) (blue), SF 704 (SECRET Cover Sheet) (red), or SF 703 (TOP SECRET Cover Sheet) (orange), whenever the documents are not in secure storage. This includes working papers. When classified material is transported from one location to another it must be covered from viewing. Protective cover sheets must not be exposed.

b. Work habits. Whenever individuals use classified information on a daily basis, there is a tendency to become careless with its protection. An individual may inadvertently place classified material and eventually store it improperly with the unclassified material. Develop work habits that will provide the appropriate security for the information, regardless of whether the information is a finished document, working paper, draft, or on a used typewriter ribbon.

c. Safeguarding and destruction of waste materials. Properly destroy preliminary drafts, carbon sheets, stencils, stenographic notes, worksheets, typewriter ribbons, and other items containing classified information immediately after they have served their purpose or provide them with the same classification and secure handling as the classified information they contain. Accomplish destruction in the manner prescribed for material of the same classification.

d. Taking classified information out of the designated working area. Classified material may not be removed from the workplace without approval of the SM. Requests for removal of SECRET or CONFIDENTIAL material from the workplace for work at home or elsewhere must be approved by the Security Office and meet all requirements identified in AR 380-5.

e. Telephone security. Individuals using a telephone in an area where classified information is frequently discussed should use extreme caution. The telephone is not a secure means of communication. Uncleared individuals can hear what you are saying! Do not discuss sensitive or classified information in an area where it may be picked up by an open telephone line. Use only secure telephones when discussing classified information. Do not let yourself be overheard during someone elseís conversation.

f. Access control. Establish procedures to control access to an area where classified information is being processed. Ensure individuals working with classified information are made aware of any uncleared visitors in the area in time to cover or protect their materials. Physical barriers provide some protection against uncleared individuals attempting to enter a sensitive area.

4-8. Emergency planning

a. Each section that maintains a security con-

tainer for the storage of classified information must develop and conspicuously display emergency destruction and evacuation plans in the vicinity of the container(s). The SOP must outline procedures designated to protect classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action. In developing emergency plans, the requirements of AR 380-5 must be met.

b. The plan should be simple, coordinated with any other offices involved, practical based on the location, type material stored, and level of threat, and reviewed and tested annually. All personnel having access to the container must be familiar with the plan and aware of their responsibilities in the event of an actual emergency.

4-9. End-of-day security checks

Heads of activities shall establish a system of security checks at the close of each working day to ensure:

a. That all classified material is stored in GSA-approved security containers.

b. Classified trash or burn bags are properly stored or destroyed.

c. Wastebaskets do not contain any classified material.

d. Ensure containers are locked and double-checked.

e. SF 702 are properly annotated by individuals locking and checking the security containers.

f. Any security container not opened during the duty day has been checked and the SF 702 annotated.

g. SF 701 (Activity Security Checklist) is annotated each day by the last person leaving the area to ensure that all precautions have been taken to safeguard sensitive and classified information.

h. Individuals are informed of procedures to follow in case a container is found open, reporting procedures, etc. (Ensure unit security SOP covers procedures.)

4-10. Classified meetings and briefings

The following is current DA policy concerning classified meetings and briefings:

a. Conduct classified meetings in a manner which best serves the interest of national security. Establish security safeguards and procedures to control access and prevent compromise of classified information presented during such meetings.

b. USAREC units or activities who sponsor classified meetings are responsible for establishing all security requirements.

c. Approval of security sponsorship of classified meetings involving attendance by other than cleared US citizens requires HQ USAREC and Headquarters, Department of the Army (HQDA), Deputy Chief of Staff for Intelligence (DCSINT) approval (nondelegable).

d. Security requirements for classified meetings are as follows:

(1) It is in the best interest of national security.

(2) Conventional dissemination channels will not accomplish the purpose of the meeting.

(3) Adequate security measures or access procedures are developed and implemented.

(4) Meeting site ensures proper physical control, storage, protection, and dissemination of classified information.

(5) DA activities accepting sponsorship of a classified meeting shall appoint a security sponsor who will ensure compliance with security requirements of:

(a) DOD 5220.22-R.

(b) DOD 5220.22-M.

(c) AR 380-5.

(d) Other appropriate directives.

e. Hold classified meetings only at a Government installation or cleared DOD contractor facility in which adequate safeguarding measures can be applied. (Hotels and motels are not authorized locations for the conduct of classified meetings.)

f. Security requirements:

(1) Meeting site appropriate for the level of classification involved.

(2) Security containers for storage of classified material available, when required.

(3) Limit access to meetings to persons whose clearance and need-to-know have been positively established.

(4) Names of all cleared or certified personnel attending classified meetings must appear on an approved access list. Entry requires positive identification.

(5) Send notices of invitations to attend classified meetings to only cleared personnel.

g. Policies and procedures governing attendance by foreign representatives and disclosures of information are contained in AR 380-10.

h. The release of classified information must be authorized in advance. Obtain authority to release classified and unclassified information not already in the public domain to foreign personnel in accordance with AR 380-10.

i. Promptly report the loss or compromise of any classified information to the unit or activity SM or the USAREC SM.

j. USAREC activities that host or sponsor events or meetings in which foreign nationals are in attendance or are participating must notify the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~, in writing, no later than 120 days prior to meeting date. Notification must include, but need not be limited to:

(1) Subject of meeting and topical outline, with classification of each topic.

(2) Date and location of meeting.

(3) Identity of sponsoring Army activities, to include: Name, grade, and telephone number of activity point of contact.

(4) Foreign countries to which the sponsoring activity desires to issue invitations, or from which requests to participate may reasonably be expected; or, fully justified proposal to exclude otherwise eligible foreign participants.

(5) Routine, recurring, in-house meetings conducted by USAREC units or activities or Government contractors related to internal operational matters, precontract negotiations, or existing contracts do not require security sponsorship provided such meetings do not involve foreign participation. All other security requirements mentioned herein, however, apply.

(6) Cited security requirements must be complied with before public announcement of a classified meeting.

(7) In addition to above cited policies, the following procedures must be followed:

(a) The sponsoring activity coordinates with their SM to plan for and apply adequate security measures for the control, issue, and storage of classified information. When classified meetings and conferences are conducted in a nonroutine, uncleared classroom, conference room, theater, or other special facility, the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ must approve the use of an uncleared facility.

(b) Control access by ensuring all personnel have been properly cleared and possess a need to know.

(c) Provide basic physical security precautions to ensure that:

1. Uncleared personnel do not inadvertently gain access.

2. Windows are covered.

3. Conversations or discussions cannot be heard outside the area where classified discussions are taking place.

4. A physical search is conducted to identify possible electronic surveillance devices present.

5. Extraneous electrical wiring, electronic equipment, and telephones are disconnected or removed from the briefing area.

(d) When classified information is going to be disclosed during a meeting or briefing, the level of the classified material must be announced and attendees advised of the consequences of unauthorized disclosure of classified information.

(e) Immediately upon completion of a classified conference, the unit or agency holding the conference must ensure that no classified material or classified waste is left in the area.

4-11. Foreign nationals

All foreign visits to USAREC activities and HQ USAREC, Fort Knox, KY, are processed through the DCSINT, HQDA, the HQ USAREC protocol officer and ~~HQ RS Bde~~ USAREC Security Office ~~Division~~, prior to any personal contact. All foreign visits to USAREC Rctg Bdes and recruiting battalions (Rctg Bns) must be coordinated with the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~. Individuals may not extend invitations or sponsor visits of foreign nationals to USAREC or supporting Army installations or activities without prior approval from HQ USAREC and the DCSINT.

a. Every effort must be made to conduct the visit at the unclassified level. Classified defense information may not be released to any foreign national without DCSINT written authorization. Verification of a foreign security clearance, to include NATO, is not to be considered authorization for release of classified information.

b. Unclassified information may be released

when requested, provided it is solely command or agency originated and does not contain information by other commands or agencies, and is approved for public release by the cognizant command or agency public affairs officer (PAO) or if the information is already in the public domain.

c. All requests for documentary information from foreign nationals acting in an official capacity must be processed through official government-to-government channels. Only those individuals who are accredited to the US Army in an attache or liaison officer capacity are authorized to formally request documentary information. Politely, but firmly, instruct visitors who request documents during the course of their official visits to initiate the request via their military attache. You may provide the visitors the title and other identifying data to facilitate any potential request providing the identifying data does not disclose classified or sensitive information.

d. Unclassified information containing the following data may not be released:

(1) Unclassified bibliographies, catalogs, and reference lists containing references to classified material.

(2) Information related to new disclosure actions or agreements until such actions or agreements are approved.

(3) Order of battle information.

(4) Cost and operation effectiveness analysis information.

(5) Third-country information, unless approved in writing by the third country.

(6) Regulations, pamphlets, manuals, etc., which may be purchased through publication channels.

(7) When classified information is authorized for release to foreign nationals only oral and visual information can be released. No information may be released in documentary form.

(8) Additional information concerning foreign visits and release of information to foreign governments can be found in AR 380-10.

(9) Address questions and assistance concerning foreign visits to USAREC and USAREC activities to the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~.

4-12. Destruction procedures for classified materials

a. What is destroyed? Destroy any document which no longer serves a purpose to the holder thus reducing the requirement for additional storage containers.

b. Conduct an annual clean-out day for destruction of unneeded classified holdings. Remember: The less you have to protect the better you can protect it.

c. The following constitutes policy for USAREC activities:

(1) Use of ìburn-barrelsî is prohibited.

(2) All classified material must be under the control of responsible individuals who are properly cleared for access up to the level of sensitivity of the material to be destroyed. Units and activities are reminded of provisions of AR 380-5. Generally, two persons are required to accomplish destruction of SECRET material and three persons (two witnesses) are required to accomplish destruction of TS material. Other directives such as AR 380-40 (O), TB 380-41 (O), and AR 380-15 (C) may also apply.

(3) A shredder is available for use in the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ for the destruction of up to SECRET material. Contact the Security Office ~~Division~~ to coordinate the destruction of material.

4-13. Disposal of unclassified paper materials

a. Paper materials for recycling may be placed in the blue recycle containers located throughout building 1307. It is recommended that For Official Use Only (FOUO) and Privacy Act information be torn into four parts prior to placement in the recycle containers. Bagged shredded paper may also be collected as recyclable material. Carbon paper must not be placed in recycle containers.

b. FOUO and Privacy Act material may also be disposed of through the recycling point but the material must be torn into four parts and placed in plastic bags or in boxes prior to deposit in the recycling bin.

c. Address questions concerning the destruction of classified material to the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~.

4-14. Changing combination on mosler hand change (MR302)

a. Lock container in locked open position.

b. Remove back cover and place on table with wheel pack facing up.

c. Slide the retaining clip off from the top of the wheel post and place it on the table. (Line up all parts in the order that you remove them.)

d. Remove the top wheel.

e. Remove the spacing washer.

f. Remove the middle wheel.

g. Remove the spacing wheel.

h. Remove the bottom wheel. (Leave the tension washer(s) on the wheel post.)

i. Set the first number of your new combination on the bottom wheel (last wheel you removed) by lining up the mark on the inner part of the wheel. Reminder: Inner part of the wheel has no lug on the back of it. Outer part of the wheel has the gate at the ì0.î

j. Place bottom wheel back on the post.

k. Place a washer onto the post and over the bottom wheel.

l. Set the second number of your new combination on the middle wheel. Inner part of the wheel has a lug. Outer part has gate at ì50.î

m. Place the remaining washer onto the post and over the middle wheel.

n. Set the third number of your new combination on the last (or top) wheel. Inner part has a lug. Outer part has gate at ì0.î

o. Slide the retaining clip back onto the top of the post.

p. Set the dial at ì50.î

q. Carefully put the back cover back on the lock.

r. Try the new combination.

(1) If it works, try it three more times before closing the container.

(2) If it doesnít work, repeat steps a through r above. If it still doesnít work, call your locksmith,

4-15. Changing combination on S & G key change (8400 and 8500 series)

a. Lock container in locked open position.

b. Cover the opening index line with your thumb or a piece of tape.

c. Dial the present combination onto the change index line. Use the normal dialing sequence except you must stop your dialing action when you come to the third number of the combination. Do not go to ì0.î

d. Insert the long end of the change key into the change hole in the back of the lock. The key must be a 6720 change key (unless otherwise specified on the back of the lock). You must insert the key according to the shape of the hole.

e. Turn the key one-quarter turn counterclockwise.

f. Dial your new combination onto the change index line. Use the normal dialing sequence except you must stop when you come to the third number. Do not go to ì0.î If you feel you made an error in the middle of the dialing sequence, start the sequence again.

g. Turn the key one-quarter turn clockwise and remove it.

h. Try the new combination.

(1) If it works, try it three more times before closing the container.

(2) If it doesnít work, call your locksmith.

SECURITY CONTAINER INFORMATION	1. AREA OR POST (If required) Fort Knox	2. BUILDING (If required) 6579	3. ROOM NO. 305
INSTRUCTIONS 1. COMPLETE PART 1 AND PART 2A (ON END OF FLAP). 2. DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER. 3. MARK PARTS 2 AND 2A WITH THE HIGHEST CLASSIFICATION STORED IN THIS CONTAINER. 4. DETACH PART 2A AND INSERT IN ENVELOPE. 5. SEE PRIVACY ACT STATEMENT ON REVERSE.	4. ACTIVITY (DIVISION, BRANCH, SECTION OR OFFICE) S-1		5. CONTAINER NO. 001
	6. MFG. & TYPE CONTAINER Mosler	7. MFG. & TYPE LOCK Mosler	8. DATE COMBINATION CHANGED 01-01-2000
	9. NAME AND SIGNATURE OF PERSON MAKING CHANGE		

10. Immediately notify one of the following persons, if this container is found open and unattended.

EMPLOYEE NAME	HOME ADDRESS	HOME PHONE
Jane Doe	111 First St., Fort Knox	999-9999

1. ATTACH TO INSIDE OF CONTAINER

STANDARD FORM 700 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

WARNING

WHEN COMBINATION ON PART 2A IS ENCLOSED, THIS ENVELOPE MUST BE SAFEGUARDED IN ACCORDANCE WITH APPROPRIATE SECURITY REQUIREMENTS.

DETACH HERE

CONTAINER NUMBER

1

COMBINATION

4 turns to the (Right) (Left) stop at 25
3 turns to the (Right) (Left) stop at 50
2 turns to the (Right) (Left) stop at 25
1 turns to the (Right) (Left) stop at 0

WARNING

THIS COPY CONTAINS CLASSIFIED INFORMATION WHEN COMBINATION IS ENTERED.

UNCLASSIFIED UPON CHANGE OF COMBINATION

2A **INSERT IN ENVELOPE**

SF 700 (8-85)
Prescribed by
GSA/ISOO
32 CFR 2003

Figure 4-1. Sample of a completed SF 700

SECURITY CONTAINER CHECK SHEET

TO (if required)	**THRU** (if required)
NA	NA

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR NOVEMBER 2000

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME
11/1	CA	0915	CA	0920	gw	0930		
11/1	CA	1310	CA	1320				
11/1	CA	1400	CA	1422	gw	1630		
11/15	CA	1030	CA	1100				
11/15	CA	1515	CA	1400	gw	1630		
11/30	CA	1400	CA	0910	gw	1630		

FOLD HERE - REVERSE FOLD FOR FULL USE OF BOTH SIDES - FOLD HERE

SECURITY CONTAINER CHECK SHEET

FROM	ROOM NO.	BUILDING	CONTAINER NO.
	305	6579	-8-

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR DECEMBER 2000

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME
12/5	CA	1100	CA	1200				
12/5	CA	1510	CA	1512	gw	1630		
12/10	gw	1010	gw	1010				
12/10	CA	1330	CA	1345				
12/10	gw	1600	gw	1610	CA	1630		

STANDARD FORM 702 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

Figure 4-2. Sample of a completed SF 702

Chapter 5
Classification

NOTE: Classification markings serve to warn the holder about the classification of the information involved and indicate the degree of protection against unauthorized disclosure that is required for the particular level of classification. It is the SMís responsibility to ensure that all classified material held by a unit is correctly marked and in compliance with AR 380-5. There are two methods of classifying national defense information, original and derivative.

5-1. Original classification

Original classification is an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required (i.e., TS, SECRET, or CONFIDENTIAL).

a. SECRET and CONFIDENTIAL. There is no original classification authority (OCA) for SECRET and CONFIDENTIAL for USAREC (AR 380-5).

b. TS. There is no original TS classification authority at USAREC (AR 380-5).

5-2. Derivative classification

a. Derivative application of classification markings is a responsibility of properly cleared personnel who incorporate, paraphrase, restate, or generate in new form, information that is already classified, or those who apply markings in accordance with guidance from an OCA. Persons who apply such derivative classifications should take care to determine whether their paraphrasing, restating, or summarizing of classified information has removed all or part of the basis for classification. Persons who apply such derivative classification markings shall (AR 380-5):

b. Respect original classification decisions.

c. Verify informations current level of classification.

d. Carry forward to any newly created documents the assigned dates or events for declassification of any additional markings.

e. When extracting classified material from one document to create another document, the extracted information shall be classified according either to the overall marking of the source, or guidance obtained from the classifier of the source material (AR 380-5).

f. ìClassified byî line: The ìClassified byî line is a part of the overall classification marking. On documents, it appears at the lower right-hand corner of the first page, title page, and front cover, if any. The ìClassified byî line must completely identify the classification authority. If more than one source is used, the term ìMultiple Sourcesî will appear on the ìClassified byî line. A complete listing of the sources used must be attached to the record (file) copy of the document. (AR 380-5).

g. Personnel creating classified material must ensure that the SM has the opportunity to review for proper document markings. Reviews must include overall markings as required by AR 380-5. This review should take place when the document is in draft form but must be done prior to dissemination.

h. îDeclassify onî line: The ìDeclassify on lineî appears directly below the ìClassified byî line. This line indicates a date or event when the material becomes declassified. If a specific date or event cannot be determined, this line will reflect ìOriginating Agencyís Determination Requiredî or OADR.

5-3. Special category material

Ensure that special category material such as 35mm slides, film, videos, automatic data processing card decks, vu-graphs, etc., are marked in accordance with AR 380-5.

5-4. Marking classified material

a. Stamp or mark the overall classification of a document at the top and bottom, on the outside front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any).

b. Stamp, mark, or affix the ìClassified byî line and the declassification instructions on all classified documents. This information should appear on the front cover, the first page of the document, on the first page of each separate appendix, annex, tab, or figure which may be separated from the document.

c. Mark interior pages of a document with the highest classification level of the information appearing on that page.

d. Individually mark major components, such as annexes and appendixes of complex documents which are likely to be used as separate documents (i.e., the first page and the back side of the last page will be marked with the overall classification of the component).

e. Mark each section, paragraph, or subparagraph to show the level of classification of the information contained within text of that portion, or to show that it is unclassified. Portions of documents are marked to identify exactly which elements are classified. Show classification levels by putting the classification symbol immediately after the portion number or letter, or when letters and numbers are not used, place symbol immediately before the beginning of the portion.

f. Mark subjects or titles of classified documents with the appropriate symbol, placed at the end and to the right of the item. When paragraphs and subparagraphs have titles or subject headings, they are marked appropriately to indicate the classification level of the information that is disclosed within the subject or title, not with the level of any subsequent paragraphs. If the information can be interpreted as unclassified when it is read by itself, then it should be marked with a (U).

g. Classification symbols are as follows: TOP SECRET (TS); SECRET (S); CONFIDENTIAL (C); Unclassified (U), and so on.

h. If a letter of transmittal, endorsement, comment, or other document is classified solely because of classified enclosures or attachments, it will be marked, ìREGRADED UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED ENCLOSURES.î

i. If a letter of transmittal or other covering document contains information of a lower level than the enclosure, it will be marked, ìREGRADED (appropriate classification) WHEN SEPARATED FROM CLASSIFIED ENCLOSURES.î

j. When classified information is upgraded, downgraded, or declassified, the following actions must be taken:

(1) Line through the old classification markings.

(2) Apply new classification markings.

(3) Mark the document with authority for the action, the date of the action, and identity of the person taking the action. When a classified document is being downgraded or declassified according to declassification instructions on the document, such markings are sufficient authority for the action.

(4) Conspicuously mark binders containing classified documents on the spine, and front and back covers.

k. Documents produced by automated systems equipment. At a minimum, mark the first page, and front and back covers, if any. (AR 380-5.)

l. Decks of automated systems punch cards:

(1) A deck of classified automated systems punched cards is handled as a single item, only the first and last card require classification markings.

(2) Add an additional card to identify the contents of the deck and the highest classification therein. Additional markings are indicated in AR 380-19.

5-5. Classified document preparation checklist

Following is a checklist for action officers and typists to use when preparing classified documents. Paragraph a lists questions to consider when preparing all types of classified documents, except messages. The checklist for classified messages is at paragraph c.

a. Consider the following questions when preparing all types of classified documents except messages.

(1) Would unauthorized disclosure of this information damage national security? (AR 380-5.)

(2) Does the information concern military plans, weapons, or operations; foreign government information; intelligence activities, sources, or methods; US foreign relations or activities; technological matters relating to national security; or US programs for safeguarding nuclear materials or facilities? (AR 380-5.)

(3) Has each paragraph and subparagraph been marked with the classification of the information in the paragraph, to include the foreign government source if it contains foreign government or NATO information? Have subjects and titles been marked? (AR 380-5.) (See fig 5-1.)

(4) Has each page of the document been

conspicuously marked or stamped with the highest classification of the information on each page? (AR 380-5.)

(5) Have I discovered a need for classifying or reclassifying the document I am working on? If so, is there an OCA in my activity who is authorized to classify the document and has the OCA approved the classification? (AR 380-5.)

(6) Was the classified information in my document extracted from another document? If so, did I fully identify (i.e., title, office symbol, and date) the source document on the ìClassified byî line? Did I use the same ìDeclassify onî date as that which appears on the source document? (AR 380-5.)

(7) Is my document classified because I extracted classified information from more than one source document? If so, have I indicated ìMultiple Sourcesî on the ìClassified byî line? Have I fully identified each of the sources used on the file or record copy of my document? (AR 380-5.)

(8) Have I classified my document for the shortest time possible and still given the classified information the degree of protection it requires? (AR 380-5.)

(9) Have I stated on the ìDeclassify onî line of this originally classified document the exact date or event on which this document will be declassified? (AR 380-5.)

(10) If my document contains foreign government or NATO information, have I shown this in paragraph markings and have I given it the longest possible declassification marking (i.e., originating agencyís determination required)? (AR 380-5.)

b. If I refer to a classified document, is my reference marked with the classification immediately preceding the document reference (e.g., AR 381-47 (C))?

c. Consider a(1) through a(10) above and the following questions when preparing all types of classified messages.

(1) Have I ensured that the ìClassified byî information is not typed in the text of the message? This information must be typed in the ìSpecial Instructionî section of DD Form 173/1 (Joint Message Form)? (AR 380-5.)

(2) Does my message have the proper declassification date or event in the last line of the text? (AR 380-5.)

(3) Have I listed the full identification of the sources that are the basis for the classification of this message on my record file copy? (AR 380-5.)

(4) If I refer to a classified message, is my reference marked with the classification immediately preceding the word ìmessageî (e.g., A CONFIDENTIAL MESSAGE), CDR, MESSAGE 052039Z, SUBJ: INCONSISTENCIES BETWEEN AR 25-11 AND AR 380-5.

RCPER-HR-S (380-5a)

MEMORANDUM FOR Commander, 28th Infantry Division, ATTN: ACofS, G2, Fort Quillen, AL 99999-9999

SUBJECT: Portion Marking (U)

1. (C) This portion of the letter is marked with a (C) following the number, to show that the lead-in contains CONFIDENTIAL information even though the contents of a subparagraph are SECRET.

a. (S) Each subparagraph carries the designation for the level of classification of that portion. In this example, this subparagraph is SECRET.

b. (U) This subparagraph is unclassified.

2. (U) References:

a. (U) FORSCOM Message, FCJ2-CIM, 311730Z Jul 99 (S), Subject: Request for Information (U). The marking after the date time group indicates that the overall classification of the reference is SECRET. An alternative is: FORSCOM SECRET message, FCJ2-CIM, 311730Z, JUL 99, Subject: Request for Information (U).

b. (U) 28th Infantry Division Letter, AXXI (C), 21 Apr 2000, Subject: Intelligence Assets (U).

FOR THE COMMANDER:

THIS LETTER CONTAINS NO CLASSIFIED INFORMATION. CLASSIFICATION SYMBOLS ARE FOR ILLUSTRATION PURPOSES ONLY.

(SIGNATURE BLOCK)

Classified by: Cdr, I Corps
Declassify on: OADR

CLASSIFIED FOR TRAINING PURPOSES ONLY

Figure 5-1. Sample of letter portion marking

Chapter 6
Transmission

NOTE: SMs are responsible for ensuring that all personnel are familiar with the correct procedures to safeguard classified information during transmission. (AR 380-5.)

6-1. Mail

a. The procedures for mailing classified material varies with the level of classification. TS material is never sent through the United States Postal Service (USPS). Whenever classified material is mailed, it will be contained in two opaque envelopes. The inner envelope will reflect the receiving activityís address, the senderís return address, and the classification of the material contained.

b. The outer envelope will reflect the addresses, but will not reflect the classification. Additional requirements must be met if the material reflects any additional protective markings (i.e., restricted data or formerly restricted data). (AR 380-5.)

(1) SECRET. SECRET material must be sent by registered mail carried by the USPS within and between the United States and its territories and by USPS express mail when no other means of transmission will meet mission requirements. (AR 380-5.)

(2) CONFIDENTIAL. CONFIDENTIAL material must be sent by USPS, first class mail within and between the US and its territories. CONFIDENTIAL material dispatched to and from US activities in Panama and Army post offices or fleet post offices addresses will be transmitted via USPS registered mail. (AR 380-5.)

6-2. NATO documents

Hand-carry all NATO classified material received from any source immediately to the SM to be brought under control. Procedures for accountability, transmission, and required access are outlined in AR 380-15.

6-3. Messages

All classified message traffic must be transmitted over a cryptographic system authorized by the Director, National Security Agency, or through a protected distribution system. (AR 380-5.)

6-4. Hand-carry procedures

Within HQ USAREC, classified information, other than message traffic, is transported by contract courier from the Distribution Center, Information Management Directorate, to the designated addressee or to the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~. Authorized personnel may hand-carry classified information from USAREC activities to other activities and from separate USAREC locations on Fort Knox, provided eligibility requirements have been met and a courier card has been issued by the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~. Prior to the issue of courier orders, every possible authorized option for the transmission of classified material will be exhausted.

6-5. Distribution systems

a. SMs must make certain that all personnel are aware that classified material is never placed inside a ìshotgunî envelope and is never sent through normal distribution channels.

b. Hand-carry classified material directly to USAREC activities or telephonically contact the responsible activity for pickup. (AR 380-5.)

6-6. Defense Courier Service

The Fort Knox TOP SECRET Control Officer and the Fort Knox Special Security Officer are the points of contact for all Defense Courier Service transactions. Refer to the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ and/or AR 380-5 for additional guidance.

6-7. Restrictions on hand-carrying classified information

Hand-carrying classified information aboard commercial passenger aircraft is approved only as an exception to DA policy. Accordingly, the policy within USAREC is that classified material shall not be hand-carried aboard commercial passenger aircraft unless there is neither time nor means available to move the information in the time required to accomplish operational objectives by other approved methods such as the USPS or other authorized courier services.

a. All requests for courier authorization by USAREC activities and subordinate units are submitted to the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ for approval. Prior to issuance of courier authorization by the Security Office ~~Division~~, the requesting organization must demonstrate that every possible option for transmission of classified information has been considered. Requests will not be approved by the Security Office ~~Division~~ merely for convenience. A sample memorandum for requesting courier authorization is at figure 6-1.

b. Prior to execution of any courier mission, the appointed individual will be briefed concerning the duties and responsibilities involved by the activity SM. A sample briefing for couriers authorized to hand-carry or escort classified material is located in the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~.

c. Designated couriers must certify they have received a courier briefing and sign a statement to this effect. A sample courier briefing certification is at figure 6-2. A copy of this statement signed by the designated courier and the activity SM must be attached to the request for courier authorization submitted to the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~.

d. Requests should be submitted to the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ a minimum of 10 days prior to travel for continental United States and 20 days prior to travel for OCONUS.

e. Written authorization for the hand-carrying of classified information on Fort Knox will be accomplished by the issuance of DD Form 2501 (Courier Authorization Card).

f. Written authorization for the hand-carrying of classified information within the US, its territories, and Canada will be approved by the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~. Written authorization will consist of a DD Form 2501 and a Courier Authorization Memorandum issued to the courier by the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~.

g. Written authorization for the hand-carrying of classified information outside the US, its territories, and Canada will be issued by the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ only after obtaining approval from the United States Army Forces Command. Written authorization will consist of DD Form 2501 and Courier Authorization Memorandum for OCONUS travel issued by the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~.

h. DD Form 1610 (Request and Authorization for TDY Travel of DOD Personnel), block 16, which indicates an individual is acting as a classified courier will not suffice as an official courier appointment.

i. Justifications for hand-carrying are extremely important since they are the basis for the approval or disapproval of the request. Justifications for hand-carrying OCONUS are forwarded to the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ as written in the request or authorization. The ~~RS Bde~~ USAREC Security Office ~~Division~~ will carefully review the request to ensure existence of an emergency situation; if not, they will not approve hand-carrying.

j. Make arrangements in advance for overnight storage in a GSA-approved container when stopovers are involved. Prepare classified material as if for mailing, double-wrap, address, and contain in a suitable package or briefcase which will be kept in the hand-carrierís possession at all times. The individual designated as the courier will have the authorized identification named in his or her letter of authorization to hand-carry in his or her possession.

k. The courier will ensure that the material is not read, studied, displayed, or used in any manner in public places or conveyances. He or she must keep the material in his or her possession and under his or her control at all times.

1. FULL NAME: Self-explanatory.

2. SOCIAL SECURITY NUMBER: Self-explanatory.

3. SECURITY CLEARANCE: Self-explanatory.

4. DUTY POSITION: Self-explanatory .

5. ID CARD NUMBER: Self-explanatory.

6. OFFICE PHONE: Self-explanatory.

7. RANK OR GRADE: Self-explanatory.

8. REASON FOR TEMPORARY DUTY (TDY): Provide the specific reason for TDY. Example: Planning conference for Exercise Troubled Water (U), briefing for USAREC unit, etc.

9. CLASSIFICATION OF MATERIAL TO BE HAND-CARRIED: Self-explanatory.

10. TYPE OF MATERIAL: Example: Briefing slides and text, OPLAN, film, etc.

11. DESCRIPTION OF PACKAGE: Provide the dimensions, in inches, of the package(s) or envelope(s). (Example: Two envelopes, 11" x 9" x 1 1/2") and to whom the package or envelope is addressed at TDY location.)

12. JUSTIFICATION: Provide specific reason(s) which precludes material from being mailed to the TDY locations. Remember, hand-carrying is an exception to policy not the policy.

13. ITINERARY: List all stops even if the courier will not debark the aircraft. Include all changes in airlines and modes of travel (privately-owned vehicle, rented vehicle, etc.). If requesting to hand-carry on the return trip, include the return trip itinerary.

14. INTRANSIT STORAGE ARRANGEMENTS: If enroute material storage is required, provide the location and facility at which it will be stored. Arrangements to do this must be made in advance and approved by the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~.

15. STORAGE ARRANGEMENTS AT TDY LOCATION: Example: GSA Security Container, HQ FORSCOM, ATTN: FCJ2-CIM, Fort McPherson, GA 30330-6000.

16. JUSTIFICATION FOR HAND-CARRYING ON THE RETURN TRIP: Describe reason for hand-carrying back to Fort Knox. This must include a description of the adverse effects on the mission if the material is mailed back to Fort Knox. Commander or director or the unit or activity security manager must sign this request.

17. PACKAGING: Package all hand-carried material in the same manner as required for mailing (AR 380-5 for packaging requirements).

Figure 6-1. Hand-carry request completion instructions

The undersigned is fully cognizant of the restrictions and responsibilities inherent to hand-carrying classified material outside of areas within military control in accordance with AR 380-5 and outlined below:

a. The unit or section security manager will maintain on file a complete list of all classified material being hand-carried.

b. Classified material will be kept under personal control or stored in a GSA-approved security container at all times or it will be locked in a GSA-approved container.

c. Do not read, study, display, or use classified material in any manner in public places or conveyances.

d. Do not leave the classified material unattended in luggage racks, aircraft travel pods, locked vehicles, car trunks, or any other unsecured location.

e. The hand-carrier will maintain the original letter of authorization to hand-carry classified material, the official military or civilian identification card (DD Form 1173 (Uniformed Service Identification and Privilege Card), or DA Form 1602 (Civilian Identification)) in his or her possession at all times.

f. The undersigned will have sufficient copies of the letter of authorization to hand-carry classified information to provide to airline or Government officials, if necessary.

g. Double wrap classified material with the inner wrapping marked to indicate overall classification and/or restrictions. Address both wrappings to the receiving station or to the hand-carrierís unit (to include office symbols), properly seal, and ensure it contains no metal bindings. No markings will be used to indicate classified or restricted material on the outer wrapping. The use of names or titles on addresses is unauthorized.

h. A locked briefcase may be used as an outer wrapping on military conveyances. However, airline officials may open the briefcase for inspection for weapons, contraband, etc. The sealed wrapping may not be opened. Locked briefcases are not authorized as an outer wrapping for travel on commercial aircraft.

i. The sealed package may be inspected by weighing, feeling, flexing, and X-raying (except for material subject to damage by X-ray). The sealed package may not be opened.

j. When contained inside a piece of carry-on luggage, aircraft or customs authorities may open the luggage for inspection for weapons, contraband, etc.

SIGNATURE OF THE COURIER _____ DATE _____

SIGNATURE OF THE SECURITY MANAGER _____ DATE _____

Figure 6-2. Sample briefing certificate

Chapter 7
Reproduction

7-1. Reproduction

Copying of documents containing classified information shall be minimized.

a. Reproduction of classified information by HQ USAREC will be accomplished in coordination with the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~.

b. Reproduction of classified vu-graphs, slides, briefing charts, and other classified audiovisual aids will be accomplished by the local Director of Plans and Training, Training Support Center (TSC). Users are responsible for complying with the TSC security requirements.

c. Commanders, primary staff officers, directors, and heads of activities must designate officials authorized to approve reproduction of classified material by position title. The ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ and the Director of Plans and Training, TSC, will be provided the full name, social security number, and signature specimen of each individual designated to approve reproduction of classified material.

d. DA Form 3964 (Classified Document Accountability Record) must be completed by the approving official for each reproduction request.

e. As an exception to the policy stated in a above, USAREC personnel who can justify a valid need to reproduce classified material on a frequent or recurring basis may submit a request to the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ for consideration. If approved, reproduction of classified material on unit copiers may not exceed 50 copies per job.

f. Sample requests for authority to reproduce classified material are at figures 7-1 and 7-2.

g. A copy of a prohibition notice, identifying officials designated to approve requests for classified reproduction, will be posted on or near each copier approved by the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~.

SECURITY
COPY MACHINE
STANDING OPERATING PROCEDURES

1. PURPOSE. To prescribe policy and establish procedures for use of the office copier to reproduce classified material as outlined in AR 380-5.

2. APPLICABILITY AND SCOPE. The prescribed policies and procedures are applicable to all personnel assigned duties with the _____. This standing operating procedure (SOP) is published as a guide to enhance and ensure security when using the copier for reproduction of classified material. Procedures set forth herein will be strictly adhered to. Any deviation is prohibited and, if any occur, immediately report the incident to the reproduction approval authorities.

3. GENERAL.

a. Reproduce no TOP SECRET (TS) material on the office copier.

b. Classified working papers or copies of classified documents reproduced for any purpose, including those incorporated in working papers, are subject to the same controls as prescribed for a document from which the reproduction was made.

c. Keep reproduction of classified documents to a minimum.

d. Do not reproduce documents bearing labels listed below without proper authority.

ìREPRODUCTION REQUIRES APPROVAL OF ORIGINATOR OR HIGHER DOD AUTHORITYî or ìFURTHER DISSEMINATION ONLY AS DIRECTED BY (APPROPRIATE OFFICE OR OFFICIALíS NAME WILL BE LISTED) OR HIGHER DOD AUTHORITY.î

4. RESPONSIBILITIES.

a. Security Manager.

(1) Ensure the warning notices are posted in the copier area along with a copy of this SOP.

(2) Ensure that TS material is not reproduced at this office. Authority to reproduce TS material, if necessary, must be obtained from the TOP SECRET control officer.

(3) Ensure the individual performing the reproduction reads and adheres to the procedures set forth in this SOP.

(4) Ensure that the copier is checked at the end of each shift, checked by the individual performing the office close-up security check, to ensure no classified residue is left in the copier and surrounding area.

b. Operators. The assigned operators are the only individuals authorized to operate the copy machine when classified material is being reproduced.

(1) Ensure uncleared personnel do not have access to classified material while reproducing classified material.

(2) Ensure that only necessary classified material is reproduced.

(3) Account for all copies including originals before leaving the machine.

(4) Ensure that all classification and special markings appear on all reproduced copies.

Figure 7-1. Sample copy machine SOP

(5) If the copier malfunctions, stay with it until the fault is corrected. Take the following steps until fault is corrected:

(a) Correct the malfunction and ensure no classified pages remain inside the copier.

(b) If malfunction is not correctable, notify the security manager, who will assist in correcting the malfunction or will notify the service representative, again ensuring that no classified pages remain inside the copier.

(c) Stay with the service representative during this entire service call to ensure access to classified material does not occur.

(d) Ensure no image remains on the image bearing surface by running a blank sheet through the copier.

(e) Prior to departing the copier area ensure that:

1. All copies are accounted for, to include the original.

2. Dispose of all classified waste, to include the blank run off sheet by shredding or storing the waste in an approved container until such time shredding or other means of authorized destruction is accomplished.

3. Enter production data on usage log, including the blank copy.

Figure 7-1. Sample copy machine SOP (Continued)

RCCS-SEC

MEMORANDUM FOR Commander, US Army Recruiting Command, ATTN: RCCS-SEC, Fort Knox, KY 40121-2726

SUBJECT: Appointment Orders - Reproduction Authorities

1. The following individuals are appointed as reproduction authorities for approving reproduction of SECRET material:

LTC John Jones
SFC Carl Smith

2. The individual desiring approval for reproduction will complete a DA Form 3964 when SECRET documents are reproduced. Approving authorities are responsible for completing DA Form 3964, section D, and will maintain them on file for a period of 2 years.

3. The point of contact for this action is LTC Jones, extension 3365.

JAMES KING
LTC, GS
Human Resources Division

Figure 7-2. Sample appointment orders for reproduction approval authorities

Chapter 8
Accountability

NOTE: The use of the term accountability in this section refers to maintaining continuous administrative control. (AR 380-5.)

8-1. Accountable

a. What material is accountable? There are five general categories of classified material for which accountability must be maintained: TS, communications security (COMSEC), NATO, restricted data, formerly restricted data, and any other material for which the originator requests accountability.

b. Continuous chains of accountability must be kept using DA Form 3964, and/or other prescribed forms, receipts, and logs. (AR 380-5.)

8-2. Nonaccountable

a. What is not accountable? US SECRET and CONFIDENTIAL material (which has no additional warning markings). Classified document custodians will not maintain accountability of these items. SMs will ensure that custodians are requiring neither signatures nor DA Forms 3964 for release of the material.

b. An informal log may be kept, but it will not be used to fix responsibility should a loss or compromise occur. Use DA Form 3964 as required for mailing purposes. Communication centers require signature for release of messages for transmission or distribution, but these are not for accountability. (AR 380-5.)

Chapter 9
Violations or Compromises

NOTE: SMs must ensure that discovery of a security violation, by anyone inside or outside of the unit, is immediately reported.

9-1. Procedures

Unit security education training must include procedures personnel must follow upon discovery of a security violation. This is mandatory and is required for a loss or possible compromise, or for an administrative violation (see fig 9-1). (AR 380-5.)

a. Discoverer. The discoverer must immediately take action, if possible, to minimize the problem. For example, securing material left unsecured and unattended or informing another individual that what he or she is doing or about to do is a violation of regulations or procedures. The discoverer notifies the unit SM immediately. The SM then advises the commander as to what action must be taken. (AR 380-5.)

b. Unit. If the situation is determined to involve a possible loss or compromise, the unit immediately initiates a preliminary inquiry and notifies the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~. When it has been determined that classified material is lost or compromised, the originator of the material must be notified. (AR 380-5.)

9-2. Preliminary inquiries

a. Appointment. If a preliminary inquiry is determined to be required, an investigating official must be appointed in writing (figs 9-2 and 9-3). Notification of appointment must be given to the appointed individual within 72 hours of discovery. (AR 380-5.)

b. Grade. The appointed individual must be a commissioned officer, warrant officer, noncommissioned officer (NCO) (sergeant first class or above), or DA civilian (GS-7 or above). The appointed official must be of a higher grade, or at least have an earlier date of rank, than the highest ranking person possibly involved in the incident and, must be briefed on responsibilities, time constraints, etc., for conducting the inquiry. The appointed official cannot be in the direct chain of command of any individual(s) possibly involved in the violation. (AR 380-5.)

9-3. Conduct of inquiry

Conducting the preliminary inquiry must be done as quickly after discovery as possible. It must be completed within 10 working days of appointment of an inquiry official. (AR 380-5.)

9-4. Sanctions

Administrative or punitive sanctions may be imposed on the individual found responsible for the violation. These sanctions range from oral reprimand to action under Article 15, nonjudical punishment. Individual(s) may face actions by courts-martial under the Uniform Code of Military Justice (UCMJ) for serious violations. (AR 380-5.)

9-5. Reporting

Submit all reports of preliminary inquiries to the appointing authority for review and corrective actions to be taken (fig 9-4). This includes the sanctions to be imposed, if any. Attach a summary of actions taken to the report. (AR 380-5.)

9-6. Review

The ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ reviews all preliminary investigations for USAREC activities prior to investigation closure.

1. References:

a. AR 380-5.

b. AR 15-6.

2. A compromise is the unauthorized disclosure of classified information. Compromises result from violations of security regulations or security weaknesses; however, not all violations or weaknesses result in a compromise. Each security violation or security-related incident must be investigated to determine if a compromise of classified information is likely.

3. The supporting security manager will notify the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ by the fastest means available of all incidents involving the possible compromise of classified information.

a. A preliminary inquiry, under the provisions of AR 380-5 will be initiated immediately upon the discovery of a possible security violation or compromise. If the compromise involves an open security container, the inquiry will include the results of an inspection of the security container for evidence of tampering.

b. The commander or principal staff officer of the unit or activity in which the security violation or security-related incident occurred will appoint a properly cleared and disinterested individual to conduct the preliminary inquiry. The appointed individual must meet the grade requirements established by AR 380-5.

c. Guidance for processing security investigations is found in AR 380-5.

d. Further investigation under AR 15-6 is authorized only after the preliminary inquiry finds that an actual compromise did occur or that damage to national security is probable, provided further investigation would clarify the causes, responsibility, or compromise aspects of the violation, or when authorized by their commander.

e. Only properly cleared commissioned officers may be appointed as investigating officers under AR 15-6.

Figure 9-1. Sample guidance for processing security investigations

S: (10 working days)

MEMORANDUM FOR (Name and Unit)

SUBJECT: Preliminary Inquiry - Possible Compromise of Classified Information

1. You are directed to conduct a preliminary inquiry concerning the facts and circumstances surrounding

2. Submit your report by endorsement in compliance with AR 380-5. Return the completed report to this headquarters no later than close of business (10 working days from date of memorandum).

3. You may obtain technical advice and assistance concerning your duties from the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ and if necessary, the Administrative Law Branch, Office of the Staff Judge Advocate.

(Signature Block of Appointing
Authority or Adjutant)

Figure 9-2. Sample preliminary inquiry appointment orders

S: _____

RCCS-SEC ( ) ( ) 1st End

SUBJECT: Preliminary Inquiry - Possible Compromise of Classified Information

(Return Address)

FOR (Appointing Authority)

1. In compliance with the appointing memorandum, the following is my report of preliminary inquiry.

2. Facts and Circumstances. (The investigating officer must be completely objective and consider all facts and circumstances to answer the following questions. When the facts are lengthy or complicated, a separate paragraph containing a narrative summary of events, in chronological order, may also be necessary.)

a. Who? (Complete identity of everyone involved, including responsible officials, and how they are involved.)

b. What? (Exact description of the information or material involved and what happened to it.)

c. When? (Date and time the incident occurred and date and time the situation was discovered and reported.)

d. Where? (Complete identification of unit, section, activity, office, building, and room number or geographic location.)

e. How? (Circumstances of the incident relating how the information or material was lost or compromised. Summarize the evidence supporting your conclusion, and attach supporting enclosures when appropriate.)

f. Why? (What are applicable policies, regulations, etc., for controlling the material or information involved? Were they followed? Was anyone negligent or derelict in his or her duties? Was the unit standing operating procedures adequate to ensure compliance with applicable directives of higher headquarters and/or for ensuring the proper protection of the information or material concerned under the circumstances?)

3. Findings. (When all of the above questions have been answered, the investigating officer should review the facts to reach findings on the following matters.)

a. Did a loss of classified information or material occur?

b. Did a compromise occur, or, under the circumstances, what is the probability of compromise, or state that a compromise did not occur, or that there is minimal risk of damage to the national security.

c. Is there any indication of significant security weaknesses in the activity or unit (i.e., were there any deficiencies in procedures for safeguarding classified information or material, or were there any violations of established procedures)? If so, were they significant or contributory to the loss or compromise?

d. Is disciplinary action appropriate? Administrative sanctions are in AR 380-5.

4. Recommendations. (The investigating officer must make specific recommendations based upon his or her findings. The recommendations may include any relevant corrective action or administrative sanctions consistent with the findings, but, as a minimum, must address the following.)

Figure 9-3. Sample report of preliminary inquiry

a. If the findings are that a loss occurred and the probability of damage to the national security cannot be discounted, or it is determined that further investigation is likely to be productive, a recommendation that an investigation under AR 15-6 be conducted may be included.

b. If there was a significant security weakness, the recommendation must include specific changes that should be made to correct the deficiency. In addition, further investigation under AR 15-6 may be appropriate if the weaknesses resulted from conscious noncompliance of applicable directives.

c. If administrative sanctions are warranted, the recommendations should identify the specific violation committed, by whom it was committed, and by whom the action should be taken. If further investigation under AR 15-6 is not recommended for one of the reasons indicated above, there need not be a recommendation for further investigation under AR 15-6 solely to impose administrative sanctions. The investigating officer should consult with the Administrative Law Branch, Office of the Staff Judge Advocate, to determine whether to recommend additional investigation or whether normal channels under the Uniform Code of Military Justice will suffice.

d. If further investigation under AR 15-6 is recommended, the recommendation should identify any person who should be designated as a respondent (see AR 15-6) and make a recommendation as to whether a formal or informal investigation should be conducted (see AR 15-6).

(Signature Block of Investigating Official)

Figure 9-3. Sample report of preliminary inquiry (Continued)

RCCS-SEC ( ) ( ) 2d End
SUBJECT: Preliminary Inquiry - Possible Compromise of Classified Information

(Return Address)

FOR USAREC Security Office

1. I have reviewed the findings and recommendations of the preliminary inquiry and concur therein (except _____).

2. I have appointed _____ to conduct an investigation in accordance with AR 15-6 and AR 380-5. - OR - In my opinion, further investigation under the provisions of AR 15-6 is not warranted.

3. Corrective actions to prevent recurrence are as follows:

4. The results of the preliminary inquiry have been referred to (responsible commander) for action as he or she deems necessary. The results of that action will be reported to you when completed.

(Signature Block of Appointing Authority)

Figure 9-4. Sample preliminary inquiry endorsement

Chapter 10
FOUO Documents

10-1. Markings

a. Information that has not been classified pursuant to Executive Order 12356, but requires withholding from the public, may be considered as being FOUO.

b. To qualify for the protective marking, the information must meet one of the Freedom of Information Act exemptions described in AR 25-55. If information does not meet the exemption criteria, it cannot be withheld from public disclosure or marked FOUO. FOUO is not authorized as a form of classification to protect national security interests.

c. Within a classified or unclassified document, mark an individual page that contains FOUO information but no classified information FOUO at the bottom of the page.

d. Address questions concerning FOUO material to the Director of Information Management.

Chapter 11
Personnel Security Clearances

11-1. Introduction

a. This portion of the SMís pamphlet is intended to provide a ready reference to procedures and instructions for requesting personnel security investigations (PSIs), security clearances, reporting adverse information on cleared and uncleared personnel, suspension of access, reinstatement of access, and designating civilian positions.

b. AR 380-67 establishes the DA Personnel Security Program (PSP) for this command and applies to all military and civilian employees of units, staff sections, directorates, and activities under command jurisdiction of the Commanding General, USAREC.

11-2. Responsibilities

a. The Commander, US Army Central Clearance Facility (CCF) is the sole authority for granting, denying, and revoking security clearances of military and civilian employees of DA.

b. The ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ has staff responsibility for management of the PSP throughout USAREC. The Security Office ~~Division~~ is the sole authority for granting interim security clearances for military and civilian personnel, requesting PSI from the Defense Investigative Service (DIS), requesting personnel security clearances or security clearance information from CCF, designation of civilian sensitive positions, reporting unfavorable information, and conducting interviews in accordance with AR 380-67 for all HQ USAREC and HQ RS Bde personnel. Subordinate Rctg Bde and Rctg Bn commanders are responsible for these actions for their respective activities.

c. Commanders, staff chiefs, directors, and activity chiefs have the responsibility for determining those positions that require access to classified defense information and material, and maintaining a sufficient number of cleared personnel to successfully complete assigned mission. Security clearance and investigative requirements are required to be established and documented for each position by the commander or supervisor of each activity.

11-3. Policies

a. Requests for personnel security actions must be routed through intelligence and/or security channels (chain of command) to the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~.

b. A certificate of clearance granted at a previous command is not valid for access until it has been accepted by the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~.

c. A clearance issued or accepted for access by the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ remains valid throughout the tenure of an individualís assignment to this command unless access is suspended by the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~, suspension is recommended by the commander or supervisor, or clearance and access is denied, revoked, or suspended by CCF.

d. SMs of USAREC Rctg Bdes and Rctg Bns are responsible for all personnel security clearance actions for assigned personnel.

e. Commanders, staff chiefs, directors, and activity chiefs must carefully review and reduce PSI requirements and requests for access by:

(1) Making every attempt to properly utilize personnel within their units who are cleared or who have a record of a complete investigation in their Military Personnel Records Jacket or civilian official personnel file. In the case of HQ USAREC personnel, the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ will verify clearance and investigative data in their Military Personnel Records Jacket and civilian official personnel file.

(2) Ensuring each investigation request is mission or job essential.

(3) Providing full justification for all requests for new investigations (i.e., single scope background investigations, National Agency Checks, and requests for access). Civilian positions must require access to classified information in performance of the job as verified by the job description and acknowledged on the SF 50-B (Notification of Personnel Action).

11-4. ~~RS Bde~~ USAREC Security Office ~~Division~~ responsibilities

a. Grant access. Personnel will not be granted access until a security clearance is issued or accepted by the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~. Civilian personnel will not be granted access unless the position they occupy is designated critical or noncritical-sensitive in accordance with AR 380-67 or, if approved by the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~, and actions are initiated to effect a change of sensitivity to a position designation. NOTE: When CCF has denied or suspended access, authority to grant access is removed from the commander or SM; only CCF may grant access in these cases.

b. Validate security clearances. Acceptance or validation of existing clearances will be in accordance with AR 380-67 and guidance provided by DAMI-CI-S and CCF.

c. Initiate security investigation and request for security clearances. Requests for National Agency Checks and single scope background investigations will be conducted in accordance with AR 380-67. New investigations must be fully justified.

d. Verification of citizenship. All requests for first-time security clearance, for a higher level of clearance or for a periodic reinvestigation (PR) with DA must contain certification of citizenship. Applicants must provide documented proof of US citizenship prior to the submission of security investigations.

e. Initiate reinvestigations. Initiate PR in accordance with AR 380-67 and CCF guidance.

f. Report derogatory information. Monitoring of cleared personnel and reporting of derogatory information will be in accordance with AR 380-67.

g. Suspend or deny access to classified information. The suspension of access or reinstatement of access and revocation of clearances will be in accordance with AR 380-67.

h. Designate civilian position sensitivity levels. Designate civilian sensitive positions in accordance with AR 380-67.

i. Foreign travel. Report foreign travel of DA military and civilian cleared personnel in accordance with AR 380-67.

j. Conduct security briefings. Provide and record initial, refresher, travel, terrorism, classified nondisclosure, and termination security briefings.

k. Grant interim security clearances.

I. Provide guidance and assistance to HQ USAREC, Rctg Bde, and Rctg Bn SMs for all personnel security matters.

m. Maintain data regarding investigative and clearance status for all HQ USAREC and RS Bde personnel.

n. Maintain, publish, and distribute security clearance and access rosters to HQ USAREC and RS Bde activities.

o. Maintain security files for all assigned HQ USAREC and RS Bde personnel.

p. Coordinate PSP issues with CCF, DAMI-CI-S, other major Army commands, Directors of Security, 902nd MI Group, DIS, Defense Investigative Service Contract Office, contractor security officers, Office of Personnel Management, civilian personnel officer, military personnel office officer, military and civil law enforcement agencies, medical facilities, drug and alcohol abuse agencies, and local commanders and supervisors.

q. Provide assistance visits and conduct security inspections.

r. Provide training and education information to commanders, supervisors, and SMs regarding the PSP.

Chapter 12
Automated Information Systems Security

12-1. Policies and procedures

a. AR 380-19 defines policy and procedures for security of automated systems, including office automated equipment (word processors).

b. Other relevant directives ~~are:~~ is

~~(1) (CRD) AR 380-19-1.~~

~~(2)~~ AR 380-5.

c. No automated system may commence sensitive operations until accredited to do so by the appropriate accreditation authority. Sensitive operations involve the processing, storage, and/or transmission of classified and unclassified national defense-related information. Complete definitions of the various types of national defense-related information are contained in AR 380-19, and the glossary.

12-2. Accreditation requirements

a. Accreditation authorities for systems designated as sensitive within the categories are outlined in AR 380-19.

b. The accreditation process is intended to cause a critical review of a system and provide information which will enable the accreditation authority to determine that sensitive information can be processed within the bounds of acceptable risk. Normally, proper documentation consists of the following:

(1) Accreditation documentation (AR 380-19).

(2) Risk management summary.

(3) Security SOP.

(4) Security official appointments (automated information system security manager, information systems security officer, terminal area security officer).

c. No automated information system requiring accreditation will commence operations until a formal, dated, statement of accreditation has been issued by the appropriate authority.

d. Provided in figures 15-1 through 15-5~~6~~ are sample forms that may be necessary using CCI and STU III equipment. Figure 15-1 is a sample CCI information paper. Figure 15-2 provides a sample of a unit property book printout of sensitive and serial-numbered CCI for the USAREC SOP. Figure 15-4 provides a sample of a completed DD Form 173/1, CCI security incident report. Figure 15-5 is a sample SOP for STU III users. ~~Figure 15-6 is a sample information paper for STU III equipment.~~

Chapter 13
COMSEC

13-1. COMSEC

AR 380-19 requires that all record communications be protected by either installation of a protected distribution system (PDS) or by encryption.

a. Protect classified information by use of telecommunications security nomenclatured encryption equipment.

b. Protect unclassified sensitive defense information by use of a PDS or commercially-developed National Security Agency endorsed encryption equipment using the Data Encryption Standard for Government systems by the Department of Commerce.

13-2. Definitions

a. To understand the above policy and impact on automated information systems engaged in networked operations, the following definitions are meaningful:

(1) Records telecommunications is the telecommunications or teleprocessing of record information.

(2) Record information is all forms (e.g., narrative, graphic, data, computer memory) of information registered in either temporary or permanent form so that it can be retrieved, reproduced, or preserved.

(3) Telecommunications include any transmission, emission, or reception of signs, signals, writing, images, and sounds or information of any nature by wire, radio, visual, or other electromagnetic systems.

(4) Teleprocessing is a form of information processing in which remote terminals access a computer via some type of communications line.

b. Those systems engaged in network operations (teleprocessing) which do not meet the requirements of AR 380-19 (PDS or encryption) must submit a request for waiver to continue operations.

Chapter 14
TEMPEST

14-1. Definition
TEMPEST is an unclassified term referring to the study of unintentional compromising emanations. ~~No computer system or word processing system may process classified information until requirements of (CRD) AR 380-19-1 have been considered.~~ The fact that an automated system has been TEMPEST approved does not exclude that system from other security requirements of AR 380-19 and any local policy.

14-2. TEMPEST control officer
The installation TEMPEST control officer in USAREC is the single point of contact for TEMPEST matters.

14-3. Procurement of TEMPEST equipment
No TEMPEST equipment may be procured without concurrence of the installation TEMPEST control officer.

Chapter 15
Telephone COMSEC Monitoring (AR 380-53)

15-1. Telephone COMSEC monitoring

a. Commanders may request COMSEC telephone monitoring to evaluate COMSEC posture of their units.

b. HQ USAREC is the sole approval authority for the conduct of conventional COMSEC telephone monitoring.

c. Requests for monitoring must be submitted to the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ 60 days prior to date required. Commanders and/or supervisors must provide:

(1) Telephone line lists.

(2) Essential elements of friendly information.

(3) Brief description of purpose for monitoring.

(4) Statement that all administrative telephones within his or her unit have DD Form 2056 (Telephone Monitoring Notification Decal) affixed to the instrument.

d. Commanders are reminded that the technique of telephone monitoring is an after-the-fact method of collecting information to evaluate the unitís COMSEC discipline. An aggressive training program that emphasizes the use of secure telephones, radios, employment of devices such as the KL 43, OPSCODES, and alerts communications systems users to the risks inherent in unprotected transmissions provides a more effective countermeasure to foreign intelligence services (FIS) signal intelligence collection.

15-2. Telephone security

a. The secure telephone unit (STU) III is a dual-function telephone. The STU III is an ordinary office telephone, used over common telephone networks. It can also secure voice conversations and data transmissions over those same common telephone networks.

b. The secure capability of the STU III is enabled and disabled by use of a removable crypto ignition key (CIK). The STU III is a controlled cryptographic item (CCI).

c. The STU III is approved for securing voice and data transmissions at all levels of classified information and categories of special access information. The type 1 low-cost terminal will replace or augment, where appropriate, all current secure and nonsecure telephones where these requirements exist.

d. Provided in figures 15-1 through 15-5~~6~~ are sample forms and reports that may be necessary when using CCI and STU III equipment. Figure 15-1 is a sample CCI information paper. Figure 15-2 provides a sample of a unit property book printout of sensitive and serial-numbered equipment. Figure 15-3 is a sample for security standards for CCI for the USAREC SOP. Figure 15-4 provides a sample of a completed DD Form 173/1, CCI security incident report. Figure 15-5 is a sample SOP for STU III users. ~~Figure 15-6 is a sample information paper for STU III equipment.~~

1. Cryptographic controlled items (CCIs) are National Security Agency approved equipment used in the encryption and decryption of information in virtually any transmission media. CCI is unclassified (when unkeyed), but has specific security control requirements for storage, access, inventory, transportation, installation, use, and incident reporting. CCI control within the Standardized Army Logistics System is very similar to the accountability, inventory, and reporting aspects of weapons and other high value, sensitive materials that require, by serial number, accountability on a recurring basis (30-day inventory).

2. Each activity security manager (SM) has specific responsibilities regarding the protection, control, usage, and incident reporting that involves CCI materials assigned or used within their area of responsibility.

3. SMs must become familiar with the contents of DA Pam 25-380-2 (FOUO). Each SM must coordinate with the activity property book officer or primary hand-receipt holder for the CCI materials assigned to their activity. The SM should know what CCI materials are held within his or her activity, and periodically become involved with the inventory process for CCI accountability (see fig 15-2). A clear audit trail should be apparent from the property book officer to the user.

4. SMs and logistics personnel should assist each other by ensuring that all CCIs within their area of concern are protected and controlled as prescribed. CCI equipment is very expensive and sensitive. The National Security Agency requires control ìFrom production to destruction.î AII CCI incidents involving loss of control, inventory irregularities, loss, theft, unauthorized access, unauthorized repair, unauthorized method of shipment, or other discrepancies require submission of an incident report.

Figure 15-1. Sample CCI information paper

LIN	EQUIP	NON/NOMENCLATURE	WAR REQ	AUTH	ON HAND	DUE IN/ ON REQ
C 52382	KY 65	Cryptographic Speech Equipment	4	4	2	2
12345	12888	(Serial numbers of two KY 65ís on hand).				
E 98103	KYK 13	Electransfer Keying Device	4	4	3	1
67166	77177	78298 (Serial numbers of three on hand).				
N 02758	KYX15A	NET CNTL Device	2	2	2	
11165	11776	(Serial numbers of two on hand).				
S 01373	KY 57	Speech Security	6	6	8	
111111	111211	13456 14456 14789 14888 15567 16667 (Serial numbers of eight on hand).				
T 40405	KOI 18	Tape Reader Gen Pur	2	2	2	
10024	10606	(Serial numbers of two on hand).				
W 60351	HYX 57	Wireless Adapter		2	2	
12345	23456	(Serial numbers of two on hand).				
211411	KL 43D	Automanual Systems Device		4	4	
20046	20123	20234 20345 (Serial numbers of four on hand). 5810-01-230-1486/87/89				
S 40645	STU III	Unit LCT TYPE 1		8	6	2
21044	33363	3876 33887 33999 40021 (Serial numbers of six on hand).				

Figure 15-2. Sample unit property book officer's monthly computer printout of sensitive and serial-numbered equipment

1. The following instructions will be used to report insecurities involving unkeyed controlled cryptographic items (CCIs) equipment. Report insecurities involving keyed CCIs, key in any form, classified communications security (COMSEC) materials or classified COMSEC equipment in accordance with AR 380-40 and TB 380-41.

2. Detailed instructions are contained in DA Pam 25-380-2. All persons that use, store, maintain, or manage CCI equipment must be familiar with the contents of that document.

3. Generally, any incident of physical loss or loss of access control under unknown or unexplainable circumstances will be reported. Minor lapses in carrying out control procedures where unauthorized access is improbable, should only be reported locally (to Director of Security) as a matter of administrative procedure. Local security managers should process and report access discrepancies. Discrepancies must be reported not later than 36 hours after the discrepancy is discovered. Disciplinary action should be considered for persons who know of and fail to report an access discrepancy.

4. Types of reportable access discrepancies:

a. Physical loss of CCIs.

b. Inventory discrepancies between an organizationís accountable property record and the physical inventory count which cannot be reconciled through recounts and causative research of supporting record files.

c. Temporary loss of access control of CCIs which are unattended, being handled, transported, or maintained.

d. Deliberate falsification of control documents, unauthorized release of CCIs, or attempts by unauthorized persons to effect such release.

5. Contents of reports:

a. Type of incident (i.e., loss, etc.).

b. National stock number, short title, serial number, owning unit.

c. As appropriate, identification (name, social security number, rank or grade, position, etc.,) of persons involved, to include the reporting organizationís point of contact for the incident.

d. The location of the incident, to include building, room, geographical location, organizationís name and address, and unit identification code.

e. A chronological account of the events which led to the discovery and verification of the discrepancy and sufficient details in the who, what, when, where, why, and how categories to give a clear picture of how the discrepancy occurred.

f. The local security managerís evaluation of the access discrepancy with an assessment as to whether unauthorized access is considered impossible, improbable, possible, probable, or certain.

6. Route all security incident reports through the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~. The ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ will review the details of the incident and make a determination as to whether a report to the US Army Intelligence and Security Command (INSCOM) is required. When it is determined that such a report is required, it will be transmitted to HQ INSCOM (IAOPS-CI-OT) for evaluation. If INSCOM determines that the access discrepancy is a COMSEC incident, INSCOM will forward the report to the Director, National Security Agency (X71) and advise the reporting unit.

Figure 15-3. Sample USAREC SOP security standards for CCI

Page 1 of 261600Z MM YY PP RR UUU 0261605Z

FROM CDR UR UNIT FT KNOX//UR OFC SYM//

TO CDR INSCOM FT BELVOIR VA//IAOPS-CI-OT//

INFO CDR FORSCOM FT MCPHERSON GA//FCJ2-CIS//

ZEN FLRO 902MIGP FT KNOX KY//IAGP-C-LE//

ZEN CDR FLWDO 6RGN CIDC FT KNOX KY//CRIFM-ZA//

ZEN CDR LEC FT KNOX KY//AFZH-PM//

ZEN (UNIT PROPERTY RECORD ACCOUNT IF NOT OWN)//

UNCLASS FOUO

QQQ

SUBJECT: CCI INCIDENT REPORT - INITIAL

A. DA PAM 25-380-2 (FOUO), 10 JAN 91, SECURITY PROCEDURES FOR CCI.

1. IAW REF A THE FOLG INFO FWD FOR YOUR EVAL AND ACTION AS REQUIRED:

A. PHYSICAL LOSS OF UNKEYED CCI, STU lll (STUGO3) 5810-01-230-1486, SERIAL NUMBER 1234, INSTALLED IN ROOM 211, BLDG 9989, FT LEWIS WA. CCI OWNED BY INSTALLATION SUPPLY SUPPORT DIV (UIC XXXX) AND ON HAND RECEIPT TO (UNIT), FT LEWIS.

B. CHRONOLOGICAL SEQUENCE OF EVENTS: AT APPROXIMATELY 0730 HRS ON 25 MAR 99, SFC DOE, JOHN E., 123-45-6789, AN NCO ASSIGNED TO TNG, DISCOVERED THE STU lll WAS MISSING FROM HIS DESK. A THOROUGH SEARCH WAS CONDUCTED WITHIN THE BUILDING AND A CHECK WAS MADE WITH ALL INDIVIDUALS THAT MAY HAVE HAD ACCESS TO THE ROOM.

Figure 15-4. Sample CCI security incident report (using DD Form 173/1)

THE DEVICE WAS UNKEYED AND VERIFIED AS PRESENT AT 1630 HRS LOCAL ON 24 MAR 99 (END OF DAY SECURITY CHECK, SF 701). THE CRYPTO IGNITION KEY (CIK) FOR THAT STU III WAS SECURED IN A GSA-APPROVED SECURITY CONTAINER WITHIN ROOM 211. THE AC POWER ADAPTER AND CONNECTION CABLES ARE ON HAND. LOCAL CIDC AND 902 Ml PERSONNEL ARE CURRENTLY INVESTIGATING THE CIRCUMSTANCES SURROUNDING THE INCIDENT.

2. WHEN FURTHER INFORMATION BECOMES AVAILABLE AMPLIFYING OR FINAL REPORT WILL BE FORWARDED.

3. POC MR GREEN, DSN 357-XXXX.

The originator is responsible for assigning the proper classification, and should examine all information furnished in the report before making a determination.

Mark reports that do not contain classified information FOUO and distribute internally on a need-to-know basis.

Figure 15-4. Sample CCI security incident report (using DD Form 173/1) (Continued)

RCCS- ____ ( )

MEMORANDUM FOR STU III Users

SUBJECT: Security Procedures for the Secure Telephone Unit Third Generation (STU III)

1. The following security procedures for STU III will be complied with by all elements.

a. When keyed the STU III will be attended by authorized person(s) with the security clearance access level equal to or greater than the classification level of the crypto ignition key (CIK). This means positive control of the keyed instrument.

b. The CIK must be secured in a GSA-approved security container when not utilized.

c. The CIK must be removed from the instrument when authorized person(s) are not present.

d. Each individual having access to the STU III must use judgment in determining ìneed to knowî when communicating classified information, and protect all notes, memos, graphs, and related papers transmitted or received.

e. Acoustical security must be taken into consideration so that uncleared or personnel not having an adequate access level do not hear the classified conversation.

f. Requirement for end of day security check of the STU III will be added to SF 701 (Activity Security Checklist) with emphasis on ensuring the CIK is removed from the STU III and properly stored.

g. Inventory of the equipment and keys will be created by each section or activity and conducted at least monthly to ensure no loss of equipment or keys. The inventory will reflect the holder and location of the key.

2. Immediately report insecurities or loss of equipment or CIK to the security manager.

Figure 15-5. Sample STU III user's SOP

Chapter 16
Physical Security

16-1. General

a. The procedures described herein are applicable to all units, activities, and personnel of USAREC and contains general guidance in areas that may be applicable to any DA activity as established in basic Army regulations. Although USAREC facilities are not directly involved with weapons, ammunitions, or sensitive item storage, information relative to these areas is provided. The principles are applicable to Government property items and include funds, supplies, equipment, and consumable or expendable supplies. Classified and medically sensitive item security procedures are outlined in other appropriate regulations, such as AR 380-5, AR 190-13, AR 525-13, and AR 190-51. Other standards may be established by the supporting installation Law Enforcement Command (LEC), Physical Security Branch, or the Installation Command Group.

b. Commanders, supervisors, and individuals responsible for the use, transport, accountability, security, or possession of Government property must take every precaution to ensure adequate security is provided for that property at all times. Throughout this chapter the term ìapproved device,î or ìsecured in an approved manner,î is used. If doubt exists, the supporting LEC Physical Security Branch or the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ determines what the approved standard will be. In those instances not clearly defined by this chapter or other pertinent regulations or checklists, commanders, supervisors, and individuals must exercise prudent judgment and employ whatever measures are available that will reasonably safeguard Government property from any possible loss, compromise, or destruction. Construction standards set forth in this regulation apply to new work, modifications, or repairs. Existing structures and standards must not be changed to conform to any regulation or policy unless approved by the supporting LEC Physical Security Branch or HQ USAREC.

c. Physical security measures employed must be adequate, reasonable, and economical. They must prevent or retard unauthorized access to information and material or equipment; and, prevent interference with the operational capability of the installation. When deficiencies exist, commanders must initiate reasonable compensatory measures until the deficiency is corrected. The submission of work orders alone may not be sufficient. In those cases where a weakness may exist, and property or equipment may be exposed, the use of constant surveillance (guards) is the best compensatory measure. Nonstandard methods and devices must be approved to ensure there is a resistance or surveillance factor equivalent to that of an approved standard.

d. Great care must be exercised to ensure security is not sacrificed for the sake of convenience. Protection of the Governmentís interest and loss prevention is the goal of this policy. Inefficiency, procrastination, fraud, waste, and abuse lead to losses or create crime-conducive conditions. Detection and prevention can only be accomplished if all concerned are alert and proactive.

16-2. Responsibilities

a. The ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ is the principle staff agency for the physical security for HQ USAREC and HQ RS Bde and provides guidance and assistance to Rctg Bdes, Rctg Bns, and support activities. Most USAREC activities are provided law enforcement support, including physical security from their AR 5-9 supporting installation. Support functions must be included in installation support agreements if specific needs are required. The following identifies functional areas that are normally associated with the principle staff agency:

(1) Maintain and update the installation physical security plan.

(2) Program and conduct periodic and annual physical security inspections and physical security surveys of the activity, mission essential/vulnerable areas and other activities, to remain cognizant of security changes or requirements impacting those areas.

(3) Manage an installation intrusion detection system (IDS). This is for the protection and security of arms, ammunitions and explosives (AA&E) and sensitive items.

(4) Provide commanders and unit physical security personnel with support and guidance on physical security matters as needed.

(5) Plan, direct, and manage the installation physical security program in its day-to-day operation, to include programming and monitoring force protection projects and funds.

b. The Directorate of Engineering and Housing (DEH) is required to ensure physical security criteria and measures are:

(1) Considered in the design, budget, and master planning phase.

(2) That work orders and projects involving security measures and equipment are coordinated with the activity and applicable security office before and during the master planning, design, budgetary, and construction or work phases.

c. The Director of Resource Management identifies fund allocations that are force protection and security related and fences them according to the security priorities set. Force protection funds should not be committed without approval of the responsible security office, the Corps of Engineers, or other action agencies.

d. The Director of Contracting (DOC) normally ensures that contracts, which are security related (i.e., lights, closed circuit television, fencing, vaults, IDS, etc.,) are returned without action if prior coordination has not been made with the responsible physical security office. Contracts or purchases related to classified material must be coordinated with the activity SM and the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ before processing.

e. The Chief of Procurement Division, Resource and Logistics Management Directorate ~~Logistics Support Center~~ should ensure that no equipment purchases for security items such as caging, safes, etc., are made without prior coordination with the responsible security office.

f. Commanders and heads of activities or units are responsible for reviewing appropriate portions of physical security regulations and USAREC publications for supplementing or incorporating its standards with SOPs and procedure guides of their own. Work orders for maintenance or purchase of security devices must always be coordinated through the responsible security office prior to submission to the DEH, Chief of Procurement Division, Resource and Logistics Management Directorate ~~Logistics Support Center~~, or DOC.

g. Unit commanders or activity managers are required to appoint, in writing, a unit physical security officer or NCO. The grade recommendations are: In the grade of staff sergeant or above, alternates may be in the grade of sergeant, civilian appointees should be in the grade of GS-5 or above, and have direct access to the commander, director, or activity head.

h. Unit physical security officers or NCOs conduct walk-through visual inspections of all unit and activity buildings, sheds, storage rooms, and areas on a periodic basis to ensure operating personnel are aware of standards and policy, and that they are in compliance with those standards. If applicable, checklists may be used when conducting walk-through inspections. Other similar inspections should be conducted before weekends and holidays to ensure the area is prepared and secure. Commanders may designate other unit personnel to conduct these inspections. Discrepancies and suggestions must be reported to the unit commander in a timely manner to ensure they can initiate appropriate corrective action. Seek advice and guidance from the supporting LEC Physical Security Branch or the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~.

i. In cases where buildings and areas are shared by multiple units or activities, one unit or activity generally assumes overall responsibility for security matters therein. This unit is referred to as the landlord. All others are referred to as tenants; and, defers to the landlord all questions of security. Landlords must establish SOPs which outline responsibilities, security measures, lockup procedures, access controls, key control, and emergency responses to bomb threats, fires, unsecure buildings, etc.

16-3. Perimeter barriers

a. A perimeter barrier is a medium which defines the physical limits of an installation, area, building, or room; and, which restricts or impedes access thereto. Perimeter barriers may be of two general types, natural or structural. The installation perimeter barriers generally consist of both types, with large portions of the perimeter being without substantial structural barriers. When needed, standard nine-gauge aluminized chain

link fencing, with a 7-foot fabric topped by a three-strand barbed wire top guard (FE-6) is used in all fencing applications. Periodic inspection and maintenance of perimeter barriers and fence lines is a normal function of the DEH. (See fig 16-1 for examples of fence details.)

b. It is necessary to define the structural perimeters of individual activities and buildings as the point at which general access to these areas is to be restricted. Periodic inspection and identification of needed repairs to these perimeters is a responsibility of unit commanders and activity heads.

c. Openings in perimeter barriers (windows, gates, doors, etc.,) must be kept to a minimum. All openings or entrances are guarded or secured when not in use. Openings, such as windows or doors, that are not needed, or necessary for emergency exit or environmental purposes, should be provided with adequate locks or be blocked or covered by screens or similar material. Other openings, such as vents and utility holes, greater than 96 square inches, through which unauthorized access to a building or area might be gained, or, into which incendiary devices might be introduced, must also be blocked or covered as necessary. Air-conditioners and vent covers must be secured to the structure. When plywood covers are used, they must be at least 1/2-inch thick or better, secured to the structure by carriage bolts. The interior ends of the bolts must be secured with nuts that are peened or otherwise secured to prevent removal. Steel bar covers are to consist of three-eighth inch steel bars, 4 inches apart with horizontal bars welded to the vertical bars so that openings do not exceed 32 square inches. Ends of the bars are securely embedded into the structure or welded to a steel frame fastened to the building by carriage bolts. Steel mesh or wire coverings must be ten-gauge expanded metal or wire mesh; or, nine-gauge chain link aluminized fencing, secured on a metal frame that is secured to the structure by carriage bolts as described above; or, by another approved method. (See fig 16-2 for an example of a standard window screen installation.)

d. As much as possible, one door to an activity is to be designated as a lockup door. This door is the first opened and the last closed.

e. Exterior doors should, as a minimum, be 1-3/4 inch solid or laminated wood, and be secured by locking devices which have a 1-inch throw deadbolt. Deadbolts will be 5/8 inches x 7/8 inches with a concealed hardened steel roller. Antifriction locksets or interlocksets with deadbolts, must conform to the ANSI A156.13 Standard. Existing doors that are secured by key-in-knob locks must have deadbolt lock sets (as described above) installed for added protection. Strike plates must use plate reinforcements that are secured with 3-inch screws. Cylinder rings must be provided with hardened steel inserts. Other exterior doors which are not solid core (with the exception of commercial aluminum and glass doors) must be secured in an approved manner (i.e., thin panels must be reinforced with plywood on interior sides; glass panels in thin wooden doors must be covered by screens or plywood). In lieu of reinforcement, paneled doors are replaced by solid core wood or metal doors. Commercial aluminum framed or steel doors, with or without glass panels, are secured by approved panic devices; mortised, heavy duty laminated hookbolts; or, other approved hardware. (See fig 16-3 for examples of approved and nonapproved locks, padlocks, and hardware.)

f. No brass shackled or brass bodied locks should be used for exterior applications on gates, doors, or in conjunction with hasps. Only approved case hardened padlocks and devices are to be used to secure Government property (except in those areas where non-spark brass is required by safety regulations).

g. Padlocks on gates or exterior doors should be protected against force by use of metal shrouds. Where this is impractical, hasps and staples should be of substantial construction and be firmly affixed to the structure or gate. Padlocks are secured to the companion staple when not in use; or, secured and controlled by the individual with the key. Padlocks and hasps are not to be used on any door which may be used for fire exit or emergency purposes. Approved panic hardware will be used in all such cases.

h. Double doors, not otherwise securely locked, must have deadbolts or canebolts (1/2-inch diameter or larger) installed on interior sides of one or both doors, top and bottom, with a minimum throw (recess) of 1 inch. Flush or extension bolts built into doors are acceptable devices, although not as strong. Dutch doors are secured in a similar manner. The use of padlocks and hasps alone is insufficient for Dutch doors. Security devices must be installed that connect the two halves of Dutch doors, as well as the top and bottom (header and threshold) of each half. The use of Dutch doors should be strictly limited.

i. An astragal of metal should be firmly affixed to the exterior of any door(s) which has a gap between the door and frame (or other doors as in the case of double doors), through which the lock or latch may be attacked or manipulated. Astragals should run the length of the door, top to bottom or side to side; but, if impractical, for the sake of cost, not less than 24 inches when used in vertical applications.

j. The use of wire mesh or chain link covers on windows or other openings (ten-gauge metal or nine-gauge chain link), is utilized to protect sensitive materials in structures and rooms. Unless otherwise specified by regulation, use of wire mesh or chain link covers should be limited if more economical means can be used (i.e., the use of key operated sash locks or sash pins) (see fig 16-4). Depending upon the threat, the criticality of the property, and the vulnerability of the activity, such screens may be necessary. Screens that are capable of swinging outward to open and to facilitate maintenance or emergency escape, will be locked in an approved manner on interior sides.

k. Panic hardware used on doors must be of the type that allows instant exit in case of emergency; however, where devices used are not lockable, they are applied only to solid doors that have no windows. Every precaution must be taken to protect nonlocking latches from manipulation. If doors are locked or chained together after duty hours, special precautions must be taken each duty day to ensure exit doors are open and functioning properly. Exit doors in troop billets or activities where personnel are working or living around the clock are not padlocked or chained.

l. The preferred panic devices are those with vertical rods (extension bars) to the top and bottom of one or both doors. With any door, the locking devices may malfunction if not properly installed. Deteriorated doors and abuse during operation are another cause. Responsible unit or activity personnel should be continually aware of the condition of doors and locks.

m. All doors, not used for lockup purposes, should be secured on the interior side by an approved method.

n. An internal lockup procedure must be implemented in each building and activity. Personnel assigned to this duty who will, at the beginning of each duty day, ensure that all doors are unlocked and prepared for emergency exit, if necessary; and, at the end of each duty day, ensure all doors, windows, and equipment are secured.

o. Exterior door, gate, or window hinges that are not already protected are required to be welded, peened, braced, or otherwise pinned to prevent easy removal.

16-4. Key and lock controls

a. All units and activities must establish minimum key and lock control measures as described below. These measures are applicable to administrative keys only. Control measures described in other pertinent regulations for sensitive items and medical or classified items have precedence. In the absence of guidance elsewhere, the minimum standard measures described herein apply in every case.

b. Administrative controls.

(1) A key and lock custodian and alternate(s) must be appointed in writing. Recommend individuals in the grade of sergeant or GS-5 or above be appointed. Custodians and alternates shall be responsible for the proper accounting and security of all keys to the activity. Persons without unaccompanied access to property and storage areas will not be appointed as custodians or alternates. In those cases where keys must be available at any time, authorized charge of quarters (CQ), SDO, or staff duty noncommissioned officer (SDNCO) may be designated to secure, issue, and/or receive keys. Under no circumstances should personnel who have been relieved of duty or who are subject or pending disciplinary action be assigned as CQ, SDO, or SDNCO duties with unaccompanied access to unit keys and property. To the greatest extent possible, CQ personnel should not be given unaccompanied access to activity or Government

property keys. Their sole function should be to provide surveillance of the area and monitor access to the locked containers in which property keys are stored.

(2) Where multiple functions exist within an activity, multiple custodians or alternates may be assigned, with separate key boxes and functions at each level.

(3) The number of personnel authorized to possess and use keys will be limited to those persons who have an absolute need, as determined by the unit commander or supervisor responsible. Persons designated to have access to a key system or separate keys therein, are identified in writing. Access forms must show the name, duty position, and key number of area authorized. The access form should be kept by the custodian or alternate who issues keys for ready reference.

(4) No keys for locks protecting sensitive Government property are to be issued for personal retention or removal from the activity. Keys for office buildings and individual rooms in troop billets may be issued for personal retention. Keys for maintenance buildings, supply buildings or rooms, motor parks, and property storage areas must be secured after duty hours in the custody of an established SDO or SDNCO; or, in an approved depository. Keys must be secured separately from all other items.

(5) All keys, when not in use, must be secured on the person of the individual to whom assigned, or be secured in a lockable container, such as a safe, filing cabinet, or key depository made of at least 26-gauge steel, that is equipped with an approved five-pin tumbler locking device or combination lock or padlock. Depositories or containers that are easily removed must be securely affixed to the structure. The key depository is to be located in a room where it is kept under surveillance around-the-clock; or, in a room that can be securely locked during nonduty hours.

(6) Portable key containers are to be secured, when not in use, in locked steel cabinets or safes. Other methods for securing portable key containers must be approved in writing by the supporting LEC Physical Security Branch or the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~. Requests for approval should be made on a standard memorandum which describes the container, the procedures in use, and the reasons for exception.

c. Accountability procedures.

(1) It should be noted that AR 190-51 makes no provision for forms use for key control. AR 190-11 does establish a form used for AA&E keys. There are three approved USAREC forms for the control and management of administrative keys by all USAREC activities. They are: USAREC Form 1191 (Monthly Key Inventory) (see fig 16-5), USAREC Form 1193 (Key Inventory Log (Monthly and Semiannually)) (see fig 16-6), and USAREC Form 1192 (Key Sign-In and Sign-Out Record) (see fig 16-7). However, this form is not required for administrative key control. All keys in the possession of a unit or activity will be strictly accounted for at all times. A complete written inventory of all keys by serial number and location is to be maintained on a master key inventory. The form is retained by the key custodian until major changes occur and a new one is made out, at which time the old form may be destroyed. (See fig 16-5 for an example of such a form.)

(2) A monthly visual inventory count of all keys in the system must be conducted by the custodian or alternate. The count is recorded on a monthly key and lock inventory form. The completed form is kept in unit files for 1 year. (See fig 16-6 for an example of such a form.) On a semiannual basis, a 100 percent serial number inventory of all keys in the system is conducted by the custodian or alternate. Personally retained keys are returned to the key custodian during each monthly inventory for accountability.

(3) Monthly and semiannual inventories of keys, to include daily changes, should be recorded on a key inventory log. It is recommended that the type of inventory be annotated in the ìtotalî block of the form. In cases where keys are maintained by the CQ, SDO, or SDNCO on a 24-hour basis, a single line entry in the staff journal indicating receipt of the number of keys is acceptable. (See fig 16-6 for an example of this form.)

(4) Keys issued for personal retention and daily use must be signed out on a separate key issue and turn-in form, which is maintained by the custodian or alternate. (See fig 16-7 for an example of this form.)

(5) A daily 100 percent visual count of all primary keys (those operational keys secured in the daily use key box or depository) must be conducted by the custodian or alternate at the start of each duty day; and, prior to any keys being issued. The inventory count is compared against the closing visual count that was annotated as the last entry for the previous day. Twenty-four-hour sign-out and sign-in logs are closed at 2400 each day. Discrepancies between the closing and opening inventory counts require investigation and resolution before issuing any keys. When closing, keys that are still out should be accounted for before closing. In those cases where the CQ, SDO, or SDNCO are securing and issuing keys on a 24-hour basis, inventories are conducted by those personnel whenever a change of custody occurs between them.

(6) Duplicate keys (extra keys not required for issue for personnel retention or daily issue) may be secured at the unitís next higher headquarters if desired; otherwise, theyíre secured in a separate container or sealed envelope or safe in the unit area. Duplicate keys may be secured with other items in the same container provided the keys are in a separate box, envelope, or similar container, sealed; and, with the quantity listed on the outside. Duplicate keys can be inventoried by container provided there is no evidence of tampering with the seal.

(7) Duplicate keys secured at the next higher headquarters, or in the unit safe, do not have to be inventoried daily, but must be inventoried by the custodians during monthly and semiannual inventories.

(8) Key control records are secured with the custodian. Key sign-out and sign-in logs may be secured in the key box or depository or in such a manner that limits or controls access to these documents in order to guard against tampering. Whiteout is not recommended for use when errors are made. Instead, errors should be lined out and initialed and the next line used.

d. Lock and combination controls.

(1) Combinations to padlocks and safe locks must be strictly controlled and protected to prevent loss or compromise.

(2) Combinations are recorded on SF 700. The information copy of the form is posted inside the container or vault, out of direct view by the public, whenever the container is open. The form may be destroyed upon change of the combination.

(3) The record copy of the combination is sealed in the envelope provided.

(4) The envelope is sealed in such a manner that allows easy detection of any attempt to open the envelope.

(5) The sealed envelope is secured at the next higher headquarters.

(6) In case of loss, theft, or compromise of a lock or combination, the lock and/or combination must be changed. In addition, changes of combinations occur annually; or, upon relief or rotation of the person possessing the combination. Lock rotation or replacement should be considered under similar circumstances.

e. Locking devices, padlocks, and hasps. (See fig 16-8 for examples of such devices.)

f. Lock replacement or repair must be identified by the unit on a DA Form 4283 (Facilities Engineering Work Request) to the supporting DEH.

g. With the exception of utility room access, the use of master keyed locks and set locks for the security of Government property is prohibited. In the case of existing buildings (such as troop billets), where master locking systems may have been installed, office doors and supply rooms in those buildings should have the locks changed to ensure Government property areas are on a separate key system from that of personal property and rooms. CQ personnel must not be given building master sets for Government property unless a clear and immediate mission requires it. The commander, SM, Director of Resource Management, and DEH should take every measure that no future installation of locks use a master key system involving Government property areas. In troop billets, personal room locks may be individually keyed and mastered to the building master only.

16-5. Building security checks

a. The unit or activity physical security officers or NCO must perform security checks of storage and unit areas on a periodic basis.

b. After duty hours, unit or activity security per-

sonnel (CQ, SDO, SDNCO) should perform periodic security checks of all unit or activity buildings and storage areas at least once every 8 hours. All such checks are recorded or logged.

c. When closing a building at the end of a duty day, designated persons make a security check of the building to ensure all doors, windows, and other openings are properly secured. SF 701 is posted at the lockup door.

d. All buildings used principally for the storage of Government property must have an emergency notification card posted on all entrances of the building or on gates leading to the building. Notification cards should not be smaller than 3 inches by 5 inches and have the following printed thereon:

ìIN CASE OF EMERGENCY NOTIFY
___(Unit)_____ TELE#_____.î

e. Notification cards must not contain the name, address, or home telephone number of responsible personnel. Unit, CQ, SDO, SDNCO, or police numbers are the only numbers used. In the case of police notification, the unit must coordinate with the police department before using that number on a notification card. Police numbers are not to be used for buildings or activities that do not store sensitive items or funds; or, which have military personnel assigned as CQ, SDO, or SDNCO. In case of emergency, only CQ, SDO, SDNCO, or police personnel call responsible personnel, who in turn, before responding, calls back to verify the existence of an emergency.

f. Emergency notification numbers of responsible personnel are not to be given out over the telephone to unknown persons or callers.

16-6. Personnel access and control

a. Unknown visitors in work areas, spaces, rooms, or buildings are to be challenged as to their direction and intent. No such individuals should be allowed free access to the facility or area, or to find their own way. They must be challenged and escorted to a supervisor or where their access need can be verified.

b. Activities should arrange office spaces (if possible) to ensure active public entrances or gates are under surveillance, and that visitors can be challenged or greeted upon entry. Public areas, such as snack and vending rooms, should be controlled or be under observation to the greatest extent possible.

c. Contract janitors or vendors should not be allowed unaccompanied access to activities or buildings after duty hours unless accompanied by authorized activity personnel. Contract janitors should not be given installation or activity keys under any circumstances.

16-7. Material control

a. All personnel and vehicles (or other conveyances) are subject to search by security personnel upon entering, traveling within, or upon exiting a Federal installation. Such searches are conducted only when authorized by the installation commander, based upon a specific security need.

b. Spot checks of trucks or other conveyances may be made for unauthorized explosives, incendiary devices, contraband, or Government property either upon entering, traveling within the installation, or upon exit. Such inspections or checks must be authorized by the commander responsible and must be based on a valid security threat.

c. Commanders or supervisors working with vendors or contractors provide such persons with adequate guidance concerning the security of their property and that of the US Government. Care must be taken to ensure that contractor property is not mixed with Government property. Areas should be designated for the consolidation of contractor tools and materials. Security of contractor construction sites must be provided for in contractual agreements, and should include direction for the marking and recording of serial numbers, registration procedures, on-site security guards, lighting, and fencing for the site.

d. Government property should never be removed from an activity without proper documentation or authorization, such as hand receipts, property pass, or other similar documentation. Responsible officials must ensure drivers, or other individuals in possession of Government property, obtain the proper documentation prior to exiting the installation. These conditions may be exempted during military unit training conditions.

e. Hand receipt holders and/or operating personnel must be cognizant of the condition and disposition of property in their area on a daily basis. Visual inventories should be conducted each duty day and at the close of business before weekends or holidays. Failure to be aware of what property is present, its condition or location; or, to see it only during periodic inventories, invites losses and makes timely detection of losses more difficult. Commanders, supervisors, NCOs, and managers must become active and aggressive with property control and security. AR 710-2, outlines the Command Supply Discipline Program. Commanders, supervisors, NCOs, and managers responsible for property should become familiar with this program.

f. Government property, that is excess, expendable, or consumable property and, items which may otherwise appear to be of no value, cannot be disposed of or be given away to private or Government personnel, except as authorized in appropriate regulations.

g. Personnel responsible for loading cargo must ensure that only authorized material is loaded and shipped. Supervisors should make spot checks of cargo or shipments to ensure theft or substitution does not occur.

h. Classified shipments must be handled in accordance with AR 380-5 and other applicable regulations.

i. Locks and seals are to be used on all shipments to the greatest extent possible. Seal accountability must be in accordance with AR 190-51.

16-8. Package control

a. All packages or hand-held items are subject to search before entry or exit from buildings or activities. Such searches must be authorized by the commander responsible and must be based upon a valid security threat. Search procedures must be delineated in writing and approved by staff judge advocate.

b. US mail or classified shipments are excluded from search if properly marked, sealed, escorted, or otherwise identified in documentation.

c. Commanders and heads of activities are responsible for establishing package controls to minimize the loss of property, and to preclude sabotage and/or espionage.

d. Activities should provide procedures for the control and restriction of employee-owned packages at the workplace (excluding lunch items). Employees should, upon entering and upon leaving the workplace, inform supervisors of the contents of privately-owned packages brought into the workplace. Activities should provide suitable and secure locations for personal lockers and package storage areas.

16-9. Vehicle control

a. Government-owned or -leased and military vehicles are to be used for official purposes only, and are not to be used by operators or responsible persons for any other purpose. Such vehicles are not to be used without proper authorization or dispatch; nor, are they to be used for personal trips to the PX, clubs, or other commercial activities. When parked, such vehicles must be secured with an approved locking mechanism or device, and the ignition keys secured in the possession of the responsible person or dispatch office. All windows, if any, are to be rolled up and locked. If padlocks or chains are used to immobilize steering wheels, only approved devices are to be used.

b. Privately-owned vehicles (POVs) must be registered on the installation or have proper permits or passes as required.

c. Under normal conditions, POVs are not to be parked within activity work areas, motor pools, or within fenced yards reserved for Government vehicles. To the greatest extent possible, POVs must be restricted from parking in or near entrances, doorways, or loading docks or work areas.

16-10. Pilferage control

a. Commanders and supervisors should ensure one individual does not have control over all transactions; such as, shipping, ordering, receiving, and transport. Limit blanket purchase authority. Ensure blanket purchase authority officials do not also control inventory and accountability.

b. Ensure trash disposal activities are monitored.

c. Employ spot checks for cargo vehicles.

d. Mark all tools and high value equipment as US GOVT or US PROPERTY. The practice of hot branding vehicle tires or the use of paint to

mark tires is not authorized. A yellow, chemically self-vulcanizing label marked US GOVT (NSN 2640-01-108-7256) will be used.

e. Employ frequent unannounced inventories of property and records.

f. Establish effective package controls for employees.

g. Prevent employees from parking POVs near doorways and docks.

h. Establish appropriate perimeters and control of gates and doors.

i. Investigate actual or suspected losses immediately.

16-11. Signs

a. Conditions of entry and warnings pertaining to search and seizure while on the installation are normally posted at entry control points of the installation boundary.

b. To minimize unauthorized entry or trespassing and to assist in the prosecution of offenders, the boundary of the installation will be clearly posted with signs at such intervals that at least one sign be visible from any approach to the boundary.

c. Restricted area signs are not to be used unless authorized by the appropriate regulation or as designated by the commander. To prohibit entry to areas where use of the term ìRestricted Areaî is not authorized, use the ìUNAUTHORIZED PERSONNEL KEEP OUT,î instead.

d. Storage areas and buildings are to be posted with appropriate signs directing visitors to the proper entry point.

16-12. Protective lighting

Protective lighting is a primary aid to security. The degree and intensity of lighting varies according to circumstances and locality. As a general rule, the following should be considered:

a. Lights of sufficient intensity at main gates and entrances that are controlled by security or responsible activity personnel.

b. Lights over all lockup doors.

c. Lights for restricted areas and sensitive item storage.

d. Lights along remote buildings and interior fence perimeters; and, in parking lots for crime prevention purposes.

e. Exterior lights on buildings that are exposed to breakage will be provided with lens covers or screens.

16-13. Security of funds

a. Supervisors of activities that handle, store, and transport funds are responsible for all such funds and must take precautions to ensure the protection of those funds. This includes, but is not limited to the following:

(1) Adequate storage sites and containers with limited access to fund storage areas and key control.

(2) Adequate cashierís cage or disbursement point.

(3) Adequate armed guards and procedures for the transportation of the funds and negotiable instruments.

(4) IDS for fund storage sites and duress alarms for cashiers with IDS signs posted on the entrance to the alarmed room. Signs are posted on exterior walls only if the alarmed area or room has an exterior wall.

(5) No mingling of funds between cashiers; or mingling of official funds with coffee funds in the same container or cash box. Cash cannot be stored in containers securing classified material.

(6) No slush fund with which overages or shortages are made up.

(7) Proper fund custodians appointed with separation of functions and or access.

(8) Written authorization for change funds and size thereof.

b. The following minimum measures should be in effect for all activities that store cash or negotiable instruments on their premises on an overnight basis, unless otherwise provided for in other regulations.

(1) All funds, that are secured on an overnight basis, that are appropriated funds or are nonappropriated funds, in excess of $200, are secured in a tool-resistant safe that is provided with a built-in three-position dial combination lock that is equipped with a relocating device. GSA-approved security containers with Underwritersí Laboratory (UL) tool-resistant ratings of UL-15 or higher may be used. If tool-resistant money safes are not available, GSA-approved Class 1 through 2, two-drawer security file containers may be used for the security of funds that are not in excess of $500. GSA-approved Class 3 through Class 6 security file containers, weighing in excess of 750 pounds, are to be used for the security of funds that are over $500, but not in excess of $3,000. Security file containers are authorized for fund storage only when there are no better containers available and when purchase of new tool-resistant containers would not be cost effective. See figure 16-8 for examples of security containers and UL ratings. Fund containers must be secured in a locked room or building of a secure storage structure as described in AR 190-51; or, be in a room or structure that is under constant surveillance of duty personnel.

(2) Funds that are less than $200, that are to be secured on an overnight basis, must be secured in an approved, lockable safe or steel container. Safes and containers that cost more than the amount of money being secured within should not be purchased solely to conform with this guidance. Two-drawer Class 1, 2, and 6 security containers and Army field safes with built-in combination locks should be used for funds in these amounts. The storage containers must be secured in a lockable room of a lockable structure or building. The use of small portable cash boxes to secure overnight storage is generally prohibited. When portable cash containers are used during duty hours, such as in dining facilities or at nonappropriated funds cash collection points, and will be kept under the control and surveillance of the cashier. When not in use, or when business is completed, the boxes are to be locked by padlocks or built-in locks, and further secured in approved safes or containers in an approved structure as described in AR 190-51. If doubt exists, the supporting LEC Physical Security Branch or the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ should be contacted.

(3) Padlocks should never be used to secure fund safe doors after nonduty hours.

(4) All safes weighing less than 750 pounds must be secured to the structure by approved methods. Hardened steel padlocks are approved for use. One method is to secure the safe to the structure by use of steel eye-bolts anchored in the floor, with short lengths of chain (5/16 thickness) beneath the safe that are secured to the anchor by steel padlocks; or, by welding the safe to the anchor. Safes that are on wheels must have the wheels removed or be bolted or secured to the structure in an approved manner.

(5) Approval to secure appropriated or private business funds in Government offices or buildings must be obtained in writing from the installation finance officer. Funds are to be kept to a minimum when overnight storage is necessary; and, only in those amounts necessary to support a change fund. Fund custodians ensure that adequate measures are put into effect to have all cash receipts or other negotiable instruments, that are not authorized for overnight storage, deposited without delay.

(6) Structural and security standards must be approved by the supporting LEC Physical Security Branch or the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ before funds are secured on an overnight basis.

(7) All fund safes, cashiers, and register points with change funds in excess of $200, should have a duress alarm installed for their use. Full IDS should be considered for any site storing in excess of $500.

(8) Keys and combinations to locks and fund safes must be safeguarded and controlled as discussed previously. SF 702 must be affixed to each fund safe, and annotated each time the safe is opened and closed.

(9) Safes shall be secured in rooms with lockable doors. Windows and other openings must be limited. If needed, such openings are to be locked, covered, or sealed in an approved manner.

(10) Authorized signature stamps or dies validating stamps or indicia plates used to certify or authorize checks or money orders must be accounted for at all times; and, be secured in the fund safe or other secure container at the close of business each day. Blank checks, money orders, or bonds must be secured in a burglar-resistant safe, vault, or container. If such safes, vaults, or containers are not available, a Class 3 through Class 6, four-drawer security file or container must be used. Books of accounts, vouchers, and related financial paperwork may be secured in the same container as the items described in this paragraph, in separate drawers or files; or, be secured in other lockable containers or field safes.

(11) Responsible officers or fund custodians coordinate with the installation finance officer to

have a cash verification check conducted as appropriate.

16-14. Tactical radios and communications equipment

a. Unless specified in writing by the commander, tactical radios and portable communications equipment must be secured in the following manner.

(1) Locked in a secure building or vehicle as described AR 190-51; or

(2) Secured to a vehicle by a 5/16-inch chain and approved padlock; or, secured by another means. The vehicle must be parked in a locked motor pool surrounded by a fence and lighted with a posted guard for surveillance. Classified or sensitive components must not be secured outside with the radios and vehicles unless constant surveillance is provided, and a specific mission requirement exists. Outside of motor park areas, unsecured tactical vehicles with radios and communications equipment on board are not to be left unattended overnight unless a specific mission exists as designated by the commander responsible. Accessory items that are easily removed (such as hand mikes) are to be stored in a locked box or compartment that is secured to the vehicle or in a secure storage building.

(3) In field conditions, responsible individuals are to maintain control and surveillance of the items in their possession. In consolidated areas or vehicle parks, commanders must ensure that operators or guards are placed to control access to the vehicles or communications items.

b. During transport by commercial means, commanders coordinate with the transportation office to ensure maximum consideration is given to proper packing and protection of shipments, particularly those that are not under surveillance or military control.

16-15. Computer and business machines security

a. Desktop computers, calculators, typewriters, and similar machines are desirable objects and are highly susceptible to theft. Every effort must be made to ensure adequate security for such items.

b. All such items are to be accepted on hand receipt by a responsible person within each office or activity. Frequent serial number inventories (not less than quarterly) should be conducted for those items that are physically located in storage or in buildings or activities. Operating personnel should conduct visual inventories daily. Consideration should be given to marking all items as US Property, for easy identification in case of theft. Caution should be exercised to ensure electrostatic engravers are not used, since they might damage sensitive microcomponents of the computer.

c. The buildings in which such items are stored or used must have adequate doors, windows, and locks. If located in rooms with lockable doors, the doors must be closed and locked at the close of business. If structure doors and windows are not up to the minimum standard, and lockable office doors do not exist, computers, disk drives, printers, and high value typewriters such as IBM selectronics and other similar machines are to be secured in containers (locally fabricated or commercially purchased). In lieu of containers, anchor pads or similar devices may be used to secure the machines in place to retard theft. Cable security devices should only be used on low value typewriters, such as manual machines, calculators, and computer peripherals such as modems and keyboards.

16-16. Organizational clothing, equipment, and personal property

a. Such property belonging to soldiers who are absent from the unit (leave, TDY, absent without leave, hospital, etc.,) are to be secured in the following manner:

(1) Property is collected and inventoried by unit officers or NCOs designated by the unit commander.

(2) Organizational or Government items are inventoried against the individual property or clothing records. Personal property is inventoried by item, quantity, description, and serial number (if any); and, recorded on a blank sheet of paper or other format if desired. The inventory record is signed by the person conducting the inventory and the owner (if present). One copy of the inventory is kept in the individual clothing record file, and one copy is given to the owner.

(3) All items are to be secured in a locked bag, wall locker, or similar container that is further secured in the unit supply room or storage room designated for such items. Storage areas must be constructed and secured in accordance with AR 190-51.

(4) Access to the locked container or storage area must be strictly controlled.

(5) Keys to containers must be secured by the unit key custodian in a sealed envelope in such a manner that tampering will be easily detected.

(6) The sealed envelope is secured in an approved key depository or file. The envelope is opened only if an emergency exists, to conduct inventories, or upon return of the owner.

(7) Monthly, the property containers are to be inspected (when key inventories are conducted) for damage or tampering. Periodic physical inventories may be conducted if the unit commander deems it necessary.

(8) SF 702 is to be posted on containers or storage area doors to indicate access times and dates. This form is retained in unit files for 90 days upon completion.

b. Individual field equipment and similar issued items must be secured at all items when not in use. In troop billets, these items are to be secured in a locked room, cabinet, or supply room. Such items must not be secured in POVs.

16-17. Mail rooms

a. The following procedures are to be implemented for the security of mail rooms:

(1) Access control must be established and limited to unit mail personnel and the commander only.

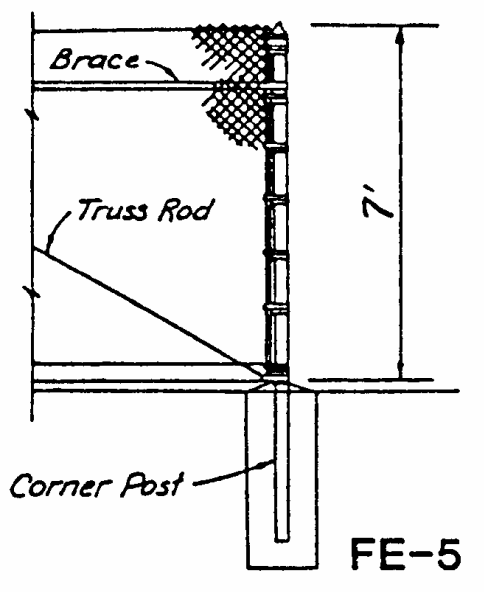
(2) Signs are to be posted on entrances to designate authorized entry only. SF 702 is to be posted on the outside of all safes and containers containing certified or classified mail and on the outside of the entrance door.

(3) Classified mail must be secured in accordance with AR 380-5.

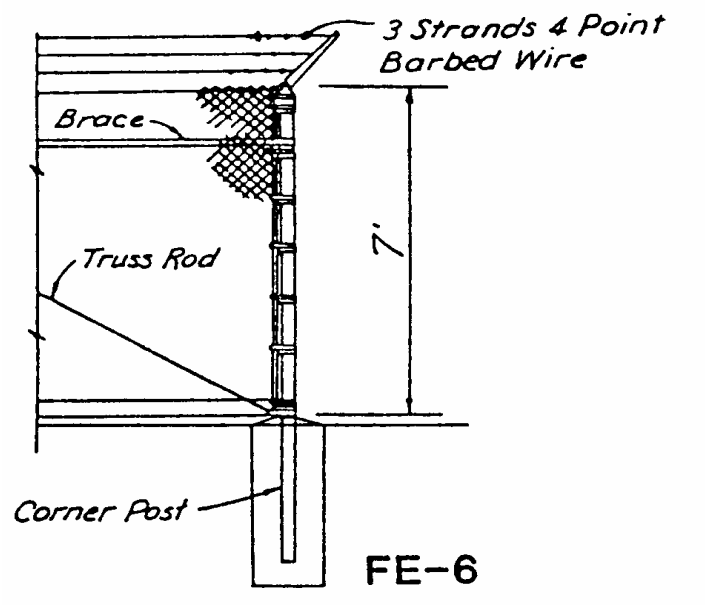
(4) Certified and registered mail as well as payroll checks, stamps, indicia, or other similar items, must as a minimum, be secured in a field safe or similar container that is provided with a built-in combination lock; or, that can be secured by an approved hasp and combination padlock. Safes or containers weighing less than 750 pounds are secured to the structure by an approved method.

b. In those cases where specific items have not been identified in this pamphlet (i.e., medical aid station items, chemical-biological-radiological storage, etc.,), commanders must use AR 190-51 as the immediate guide for determining security measures. If in doubt, coordination should be made with the supporting LEC Physical Security Branch or the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ for a determination of standards.

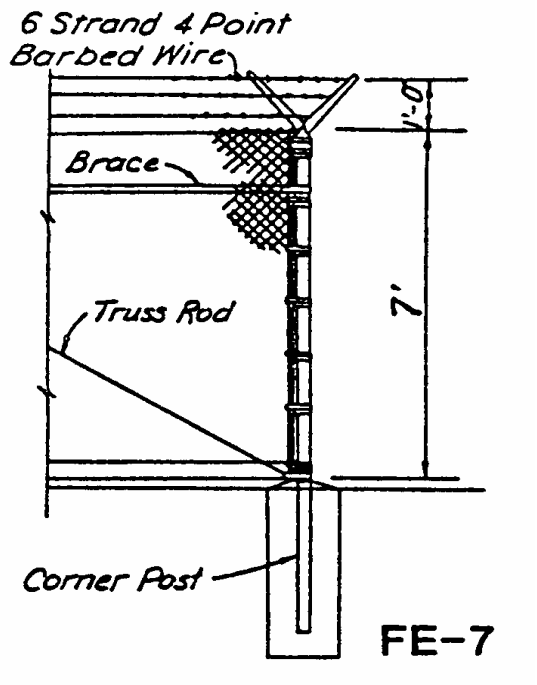
c. Commanders or supervisors must initiate investigations whenever reported losses occur, are suspected, or, whenever a storage area is subjected to actual or attempted break-in. The provisions of AR 735-5 are to be used for other property losses; or as otherwise directed by the installation or activity commander.



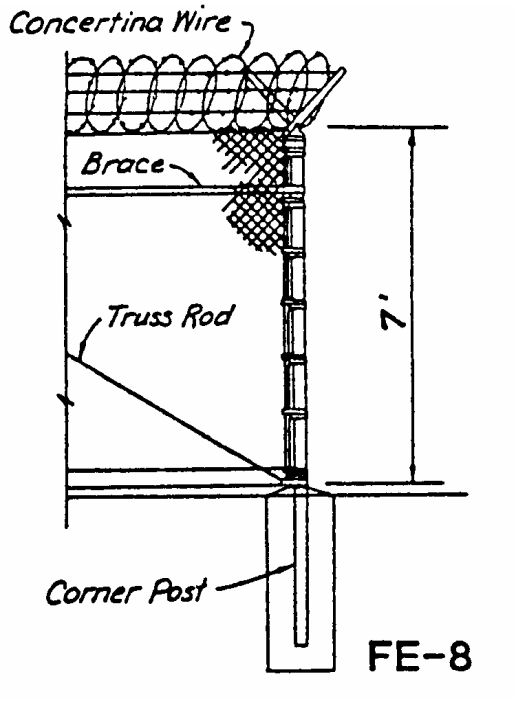
USACE Standard FE-5
No outriggers.



USACE Standard FE-6
Single barbed wire outrigger.



USACE Standard FE-7
Double barbed wire outriggers.



USACE Standard FE-8
Double outriggers with barbed wire and barbed tape.

Figure 16-1. Fence details

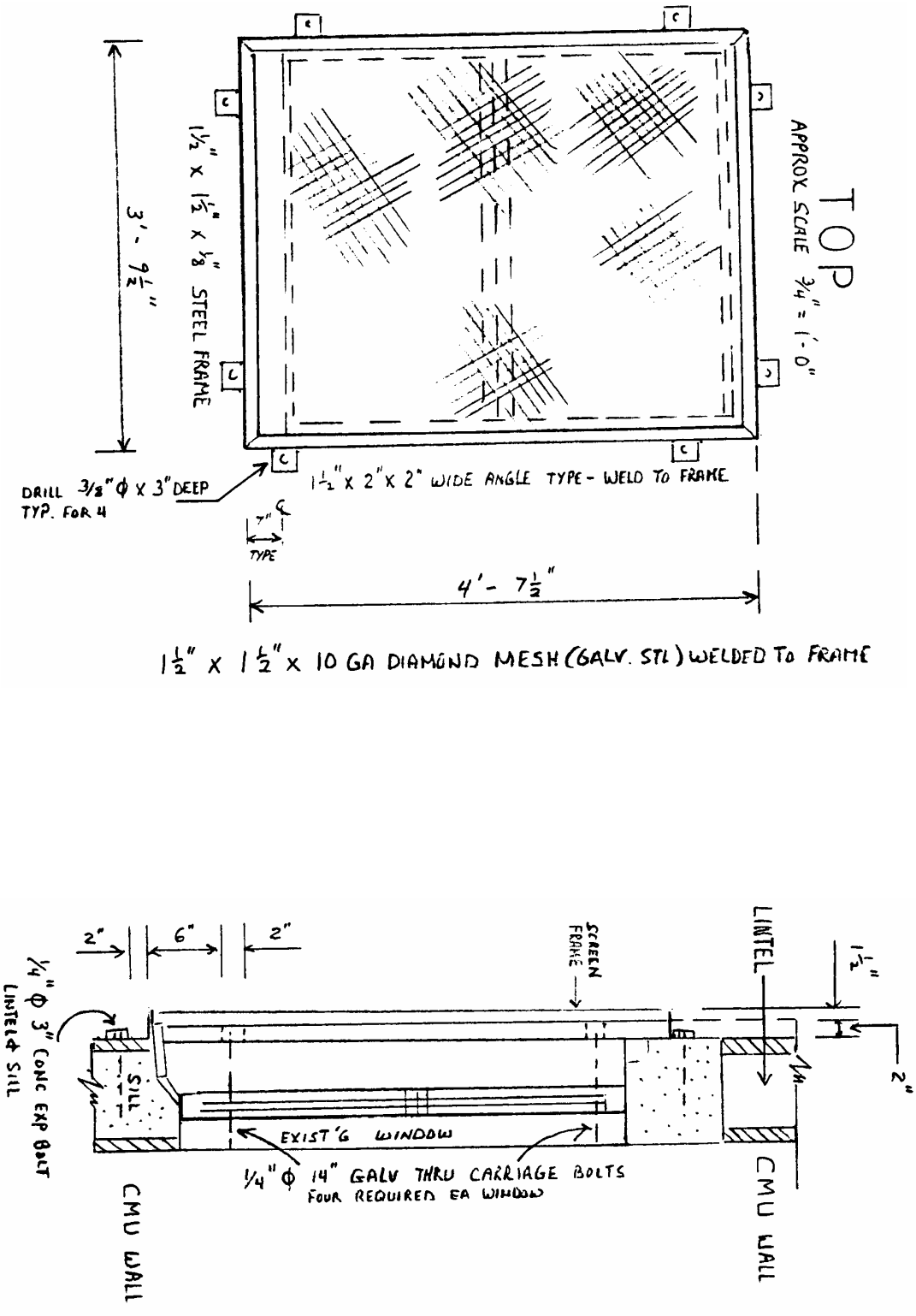
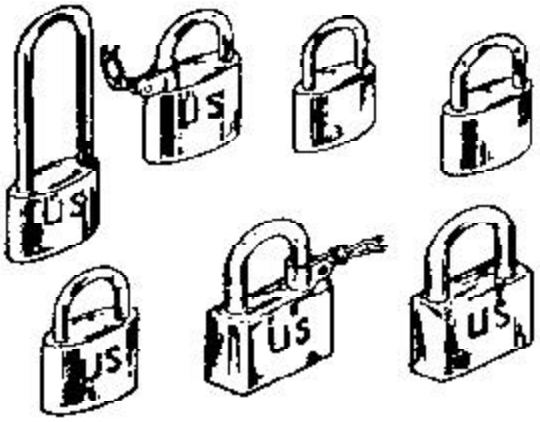
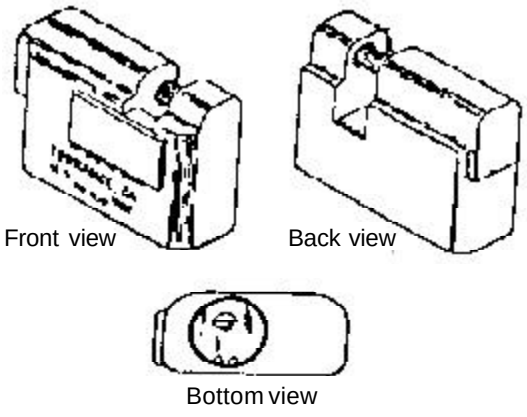


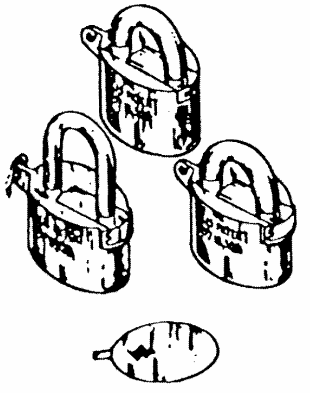
Figure 16-2. Window security screens



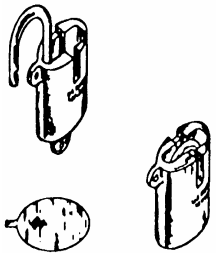
Low security padlocks



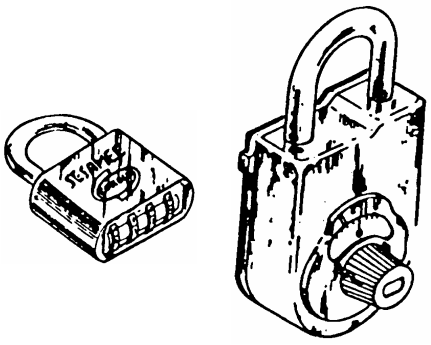
Model LK 1200 Hi-Shear High Security Padlock



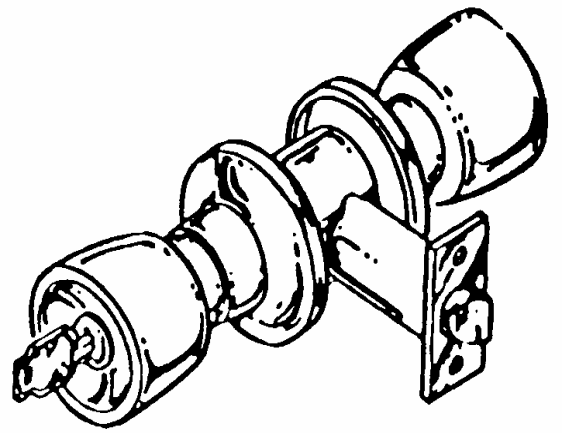
Medium security padlocks



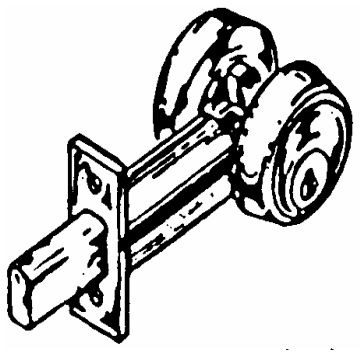
High security shrouded padlocks



Typical combination padlocks

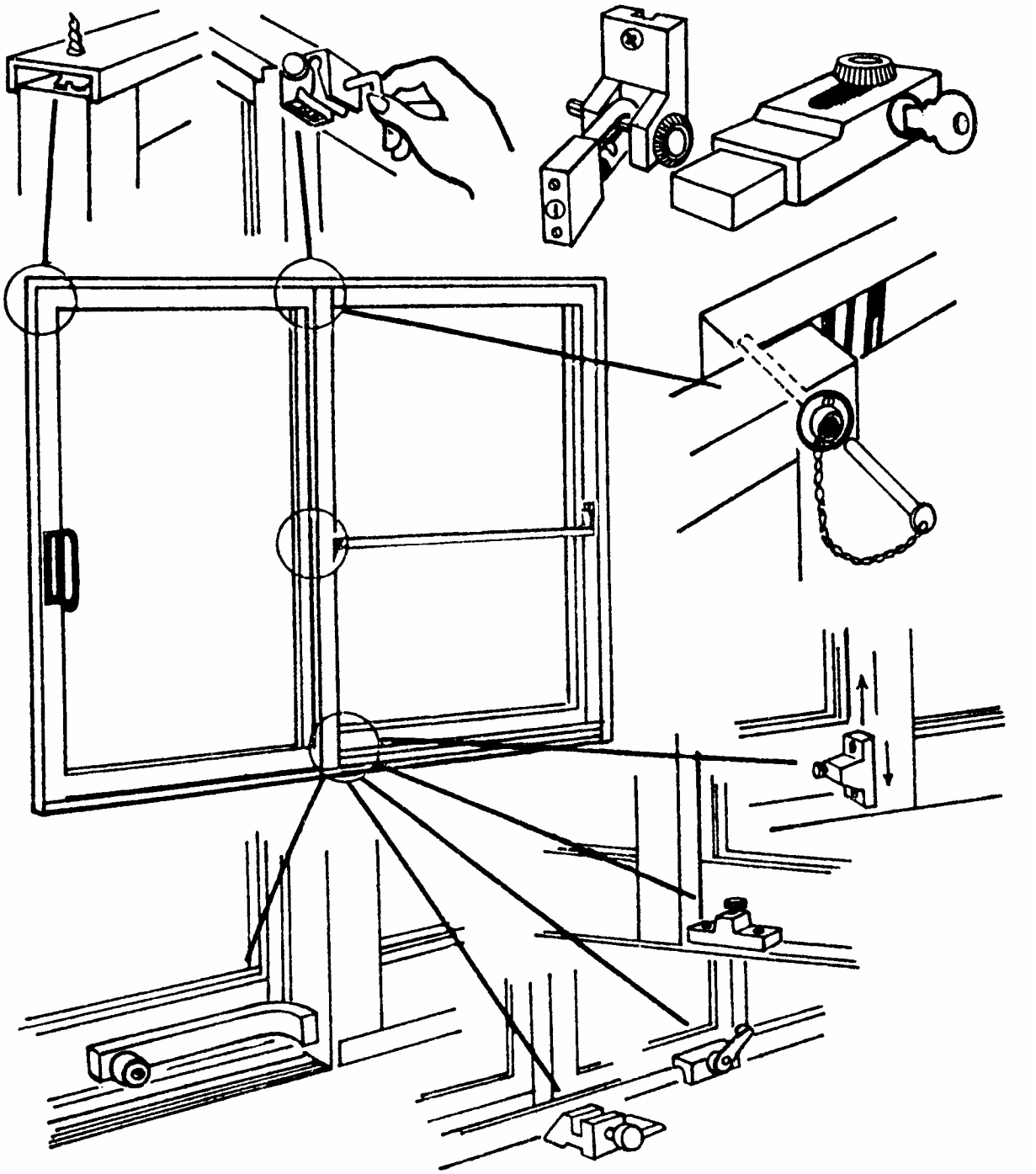


This example is a key-in-knob lockset. Most commonly used. It is recommended for internal doors only. If used on exterior doors it must be supplemented by a 1-inch throw deadbolt as shown above.



This 1-inch throw deadbolt is recommended as the minimum type of device. The above example is a double cylinder which should not be used in fire exits. Single cylinders should be used in most cases.

Figure 16-3. Padlocks and hardware



16-4. Window security devices

MASTER KEY INVENTORY

(For use of this form see USAREC Memo 190-1 and USAREC Reg 380-4)

(1) Date: 1 Mar 2000 | **(2) Office Symbol:** RCAB-SS

(3) RING/HOOK NUMBER	(4) KEY SERIAL NO.	(5) LOCATION OF LOCK	(6) PRIMARY KEYS *(No. in Box)*	(7) NO. OF DUPLICATE KEYS	(8) TOTAL KEYS
1	R0612	Bldg 110/Rm 3	1	6	7
2	081361	Bldg 110/Rm 5	1	3	4
3	01123	Bldg 110/Rm 7	1	3	4
4	061124	Bldg 110/Rm 9	1	3	4
5	0113	Desk Rm 9	1	2	3
6	0114	Desk Rm 7	1	2	3
7	0115	Desk Rm 5	1	2	3
8	0116	Desk Rm 3	1	1	2
9	16314	Storage Cabinet Rm 3	1	1	2
10 (a)	A1636	Bldg 110/Rm 11	1	2	3
(b)	A17999	Storage Cabinet Rm 11	1	2	3
(c)	C61	Locked Box in Storage Cab Rm 11	1	2	4
11	R1682	Key Box Rm 3	1*	3	4
12	8991	Computer Drive Rm 3	1	1	2
13	4611	Diskette Box Rm 3	1	1	2
14	3221	File Cabinet Rm 3	1	3	4
	* Key located in director's office key box in sealed envelope.				

	(9)	(10)	(11)
TOTAL	16	38	54
TOTALS *(if more than 1 page issued)*	(12)	(13)	(14)

USAREC Form 1191, 1 Feb 2000 (This form supersedes HQ USAREC Form 1871-1-R which may be used until exhausted)

Figure 16-5. Sample of a completed USAREC Form 1191

KEY INVENTORY LOG (MONTHLY AND SEMIANNUALLY)
(For use of this form see USAREC Memo 190-1 and USAREC Reg 380-4)

INVENTORY RESULTS						
(1) DATE	(2) INVENTORY TYPE MO	(2) INVENTORY TYPE SA	(3) NO. OF PRIMARY KEYS	(4) NO. OF DUPLICATE KEYS	(5) TOTAL	(6) SIGNATURE OF PERSON CONDUCTING INVENTORY
01/09/1999	X		16	38	54	
02/06/1999	X		16	38	54	
03/05/1999	X		16	38	54	
04/10/1999	X		16	38	54	
05/06/1999	X		16	38	54	
06/12/1999		X	16	38	54	
07/12/1999	X		16	38	54	
08/08/1999	X		16	38	54	
09/09/1999	X		16	38	54	
10/11/1999	X		16	38	54	
11/11/1999	X		16	38	54	
12/15/1999	X		16	38	54	

USAREC Form 1193, 1 Feb 2000 (This form supersedes HQ USAREC Form 1871-3-R which may be used until exhausted)

Figure 16-6. Sample of a completed USAREC Form 1193

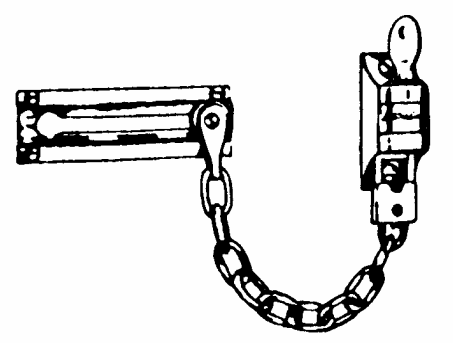
KEY SIGN-IN AND SIGN-OUT RECORD
(For use of this form see USAREC Memo 190-1 and USAREC Reg 380-4)

(1) Daily Issue: ☑ **Yes** ☐ **No** **Name:**

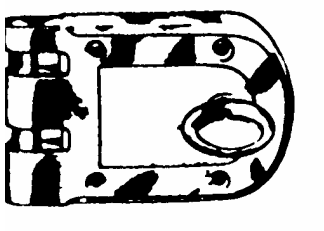
(2) RING/HOOK NUMBER	(3) DATE ISSUED	(4) ISSUED BY *(Initials)*	(5) PRINTED NAME/SIGNATURE	(6) DATE TURNED IN	(7) RECEIVED BY *(Initials)*
10	09/09/2000	JRW	JOHN SMITH	09/09/2000	JRW
4	09/09/2000	JRW	VICKI WELLS Vicki Wells	09/09/2000	JRW
2	09/09/2000	JR	JAMES JONES James Jones	09/09/2000	JR
			CLOSED 1630 09/09/2000		
			CLOSED 1630 09/10/2000		
NOTE: Closing entry.	09/11/2000		ROBERT FOIL Robert Foil	09/11/2000	
			CLOSED 1630 09/11/2000		

USAREC Form 1192, 1 Feb 2000 (This form supersedes HQ USAREC Form 1871-2-R which may be used until exhausted)

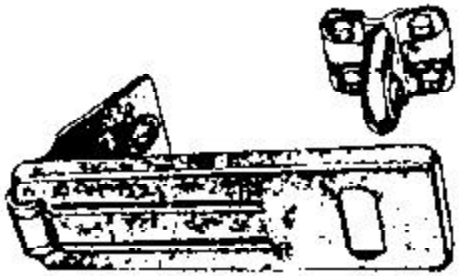
Figure 16-7. Sample of a completed USAREC Form 1192

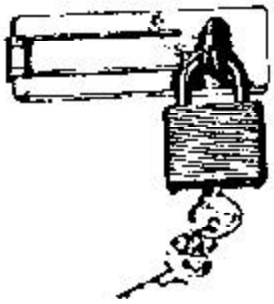


Chain locks of this type are not authorized for use in any circumstance.

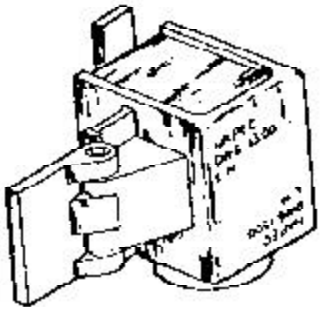


Jimmy-proof locks of this type may be used in lieu of padlocks, when approved.

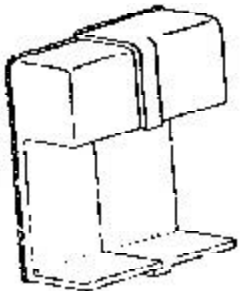




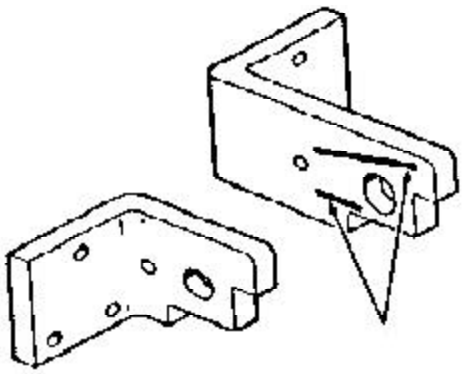
Commercial hasps, staples, and padlocks as shown here are not authorized for use.



NAPEC 1300 series high security hasp



NAPEC shrouded series high security hasp



NATICK high security hasp

Figure 16-8. Approved locking devices

Chapter 17
Physical Security of AA&E

17-1. Purpose

At the present time, USAREC activities do not, as a general rule, maintain conventional A&A, to include privately-owned weapons and ammunitions or other sensitive items such as night vision devices (NVD) that require storage in arms facilities or rooms, or alternate storage sites. This chapter is provided as a guide to maximize the protection of such items should they come into the possession of a USAREC activity and, at the same time, inform SMs of processes and procedures involved in the protective procedures for these items at a traditional activity. If there is any conflict between the provisions of this pamphlet and those of the basic regulations, the basic regulations have precedence. AR 190-11 contains minimum requirements.

17-2. Responsibilities

a. Commanders, supervisors, and/or individuals responsible for the use, handling, transport, accountability, security, or possession of A&A, to include privately-owned A&A, and other sensitive items should take every reasonable precaution to ensure adequate security is provided for all A&A and sensitive items at all times. In those instances not clearly defined by this pamphlet or other pertinent regulations, commanders, supervisors, and individuals must exercise prudent judgment and employ whatever measures are available that will safeguard A&A and sensitive items from any possible loss or destruction.

b. The supporting installation command provost marshal is responsible for the promulgation of physical security guidance and procedures for their area of responsibility (i.e., Fort Knox provides policy and procedures for HQ USAREC). A physical security inspection is conducted on a regular basis, normally at 12 to 18 month intervals, for each A&A facility or room, NVD storage area, mission essential and vulnerable areas, and any facility utilizing IDS. Normally, inspections for all other facilities will be conducted every 2 years.

c. HQ USAREC, HQ RS Bde, Rctg Bde, Rctg Bn, and directorate SMs are responsible for:

(1) Periodically inspecting subordinate units to ensure compliance with applicable regulations.

(2) Acting as a point of contact between the supporting LEC Physical Security Division and the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~.

d. Commanders should:

(1) Appoint in writing a unit physical security officer or NCO in the grade of staff sergeant or above. Alternates may be sergeants or above.

(2) Establish and disseminate security procedures and guidance throughout the unit, particularly during the training of unit personnel.

(3) Ensure the unit armorer is chosen on a selective basis, and that provisions are made to monitor his or her activities in the arms facility or room on a daily basis.

(4) Monitor all phases of A&A and sensitive item security within the unit to ensure immediate action, guidance, and supervision are provided as required.

e. The unit physical security officer or NCO should:

(1) Assist the commander by closely monitoring the unit arms room and sensitive item storage sites; and, ensure IDS tests are conducted by the unit on a monthly basis.

(2) Ensure that the unitís A&A and sensitive item security is in accordance with regulations and other applicable guidance, in particular, required inventory and accountability procedures. The supporting LEC Physical Security Division or the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ may be contacted directly for technical guidance or information.

(3) Use the checklist in chapter 20 to periodically inspect the unit arms facility or room.

f. The DEH or Corps of Engineers coordinates with the supporting LEC Physical Security Division on all construction or modification of A&A and sensitive item storage sites before such work begins, to include, when available, definitive drawings and/or specifications of the work being done.

g. The DOC ensures that contracts relating to A&A or sensitive items contain specific provisions for the security of such items, particularly during transport. The DOC also ensures that all contracts pertaining to use or procurement of commercial IDS is coordinated with the applicable security office.

17-3. Waivers and exceptions

a. Requests for waivers for AR 190-11 must be submitted to the supporting LEC Physical Security Division and the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ for coordination, concurrence, approval, and/or submission to appropriate DA agency.

b. Temporary exceptions to the provisions of DA or supplemental regulations may be granted on a case-by-case basis when correction of a deficiency is not feasible, practical, or economical, or when security afforded is equivalent to or better than that provided under the standard criteria.

17-4. Individual Reliability Program

a. Commanders must be selective in assigning personnel to duties that involve control of A&A or sensitive items. Individuals who are designated in writing by the responsible commander, and who may have unaccompanied access to A&A and sensitive item storage areas must be members of the Individual Reliability Program (IRP).

b. IRP procedures and requirements are established in AR 190-11.

c. Commanders must constantly review and be aware of the performance of IRP personnel. If any doubt exists, access to A&A or sensitive items by those personnel should be curtailed until the question is resolved.

17-5. Access control procedures for A&A and sensitive item storage areas

a. The number of individuals authorized by the commander to have unaccompanied access must be limited to the minimum number essential. Unaccompanied access must not be granted to personnel that are not members of the unit; or, who are not members of the landlord unit, as in the case of consolidated facilities or rooms where separate unit enclosures are not used.

b. The name, rank, social security number, and duty position of unaccompanied access personnel are to be listed on a memorandum. One copy of the list will be posted prominently inside the storage facility or room. Two copies of the individual unit arms room or consolidated arms room unaccompanied access roster, with emergency notification information, of which one copy will have the original unit commanderís signature, will usually be required by the supporting LEC Physical Security Division or provost marshal for use in IDS operations.

c. Personnel who are not on the unaccompanied access roster, who need entry into the storage facility or room, first reports to the unit orderly room or command post (to include inspectors and IDS maintenance personnel) where their access requirement can be verified; and, in order that they might be escorted by a designated person that is authorized unaccompanied access. Police or emergency personnel responding to alarm or emergency conditions are exempt from this provision.

d. Personnel who find a storage facility or room unsecured must immediately report this fact to the chain of command, officials identified on the posted emergency notification card, their supporting military or civil law enforcement agency, by whatever means possible, without leaving the site unguarded. Personnel are to stand by the facility or room entrance ensuring that no unauthorized entry or tampering occurs until the arrival of the unit commander or designated representative.

e. Commanders must establish a specific chain of control which ensures that no person(s), to include those authorized unaccompanied access, can gain access to the storage facility or room without first reporting to another person in the chain of control. This can be accomplished by designating specific times and periods of operation and by securing access keys at the next higher headquarters with an SDO or SDNCO.

17-6. Key control procedures for A&A and sensitive item storage areas

a. Administrative controls.

(1) A key and lock custodian and alternate(s) are appointed in writing. These persons shall be responsible for the proper accounting and security of all keys to the storage facility or room. Armorers and others whose duties require daily unaccompanied access are not to be appointed as key custodians or alternates. Only custodians and/or alternates account for keys. In those cases where keys must be available at

any time, authorized SDO or SDNCO may be designated to secure, issue, and/or receive keys.

(2) The number of personnel authorized to use keys must be limited to those persons who have an absolute need, as determined by the unit commander responsible. There will usually be only one primary set of entrance doors and joint service interior intrusion detection system (JSIIDS) or IDS operator keys or access codes in use for each arms facility or room. Duplicate sets must not be provided to other units.

(3) No keys for locks that protect arms, ammunition, or sensitive item storage areas should ever be issued for personal retention and/or removal from the unit area, except in those cases where the storage area is physically elsewhere on the installation. When not needed for official purposes at the storage area, the keys must be returned to the key depository or authorized custodian. Keys for high security locks and the JSIIDS control panel, that are broken or damaged, may not be duplicated, but must be returned to the factory for replacement, or have the lock set recored by an authorized locksmith. If keys to high security padlocks or JSIIDS are lost, the locks are required be recored or replaced.

(4) All keys must be secured on the person to whom issued, or be secured in an approved container or depository when not in use. Keys for sensitive item storage areas are to be secured in separate dedicated containers or depositories from administrative keys. Approved containers or depositories must be of at least 20-gauge steel, equipped with a pin tumbler key cylinder, or be secured by a built-in combination lock or an approved secondary padlock. Containers or depositories weighing less than 500 pounds must be securely affixed to the structure in which located, or be secured in a safe or other metal container or file that is secured to the structure, and be located in a room that is kept under constant surveillance, or in a room that can be securely locked after duty hours. The container or depository are kept closed and locked except to issue and receive, or inventory the contents.

(5) The following GSA-approved key containers are recommended for use in lieu of standard 20-gauge steel containers.

(a) Mosler Utility Locker, GS-1259, GSA Special Item #489-157.

(b) Mosler Key Locker, KL-749, GSA Special Item #489-102.

(c) Mosler High Security Key Cabinet, KC-1612, GSA Special Item #489-159.

(6) Portable key containers must be secured, when not in use, in locked steel cabinets or files or safes. Normally, other methods for securing portable key containers must be approved in writing by the supporting LEC Physical Security Division. Requests for approval should be made on a memorandum.

(7) In cases where a Rctg Bn, or a designated unit of the Rctg Bn, maintains security and accountability of the facility or room keys in a central depository, the following steps are to be observed:

(a) Users in need of the keys report to the key custodian or alternate (in some cases an SDO or SDNCO) who verifies the userís identity against the access list provided by the userís unit commander.

(b) The custodian or alternate issues the keys to the user on DA Form 5513-R (Key Control Register and Inventory). If the keys are in a unitís locked portable key container, the container must be opened by the user in order that the custodian or alternate may annotate the key ring number or individual key serial number.

(c) Whenever the key depository is opened or closed, the custodian or alternate annotates SF 702 which is affixed to the key depository. A separate SF 702 need not be affixed to each portable key box.

(d) Any change in custody of the keys prior to their storage by the custodian or alternate must be annotated on DA Form 5513-R.

(e) Upon return of the keys to the custodian or alternate, the user opens the locked unit key container, if used, to allow the custodian or alternate to verify the serial numbers and quantity of keys returned.

(8) In cases where keys are secured and accounted for at the unit level on a daily basis, but secured temporarily overnight or on weekends with an SDO or SDNCO, the keys are transferred to the SDO or SDNCO in a locked metal container or a sealed envelope, in which case, the envelope need not be opened to verify the keys. If locked containers are used without the seal, the container is opened upon issue or return in order that the SDO or SDNCO may verify the contents of the container. The SDO or SDNCO uses DA Form 5513-R or the daily staff journal to record key control transactions between themselves and the user.

b. Key inventory and accountability.

(1) All keys in the possession of a unit or activity must be strictly accounted for at all times. A complete written inventory of all keys must be maintained on DA Form 5513-R.

(2) A monthly serial number inventory of all keys is conducted by the custodian; results are recorded on DA Form 5513-R. All key inventories, to include daily changes and visual contents are annotated on this form.

(3) Keys issued for daily use are signed out and in on DA Form 5513-R.

(4) A daily 100 percent visual count of all primary keys is conducted at the start of each duty day; and, prior to any keys being issued. Discrepancies between the closing inventory count and the opening inventory count must be investigated and resolved before closing. Duplicate keys, secured at the next higher headquarters, do not have to be inventoried daily.

(5) Duplicate keys are secured at the unitís next higher headquarters in an approved key depository or file, separate from all other keys. Duplicate keys are to be inventoried by the key custodian by serial number on a monthly basis. Keys in sealed envelopes or containers can be inventoried by envelope or container provided there is no evidence of tampering.

(6) All key control records must be secured by the custodian or alternate. All entries on key control documents must be in ink. Whiteout should not be authorized for use. If an error has been made, the error is lined out and initialed and the next line used. Use of authorized computer-generated forms and data is acceptable.

c. Combination controls.

(1) Combinations to padlocks and safe locks are to be strictly controlled to prevent loss or compromise.

(2) Combinations are recorded on SF 700. The information copy of the form is to be posted inside the container or vault, out of direct view when the container or vault is opened.

(3) The record copy of the combination is placed in the sealed envelope provided.

(4) The envelope is to be sealed in such a manner that allows easy detection of any attempt to open the envelope.

(5) The sealed envelope is secured at the next higher headquarters in an approved container or file.

(6) In cases of loss, theft, or for investigative purposes the envelope is not to be opened or tampered with except by direction of the Criminal Investigation Division (CID).

(7) Combinations must be memorized by users and must not be recorded except as authorized.

(8) Combinations are to be changed annually; or, upon loss, theft, compromise, or upon relief or rotation of the person possessing the combination.

d. Locking devices and padlocks.

(1) Sargent and Greenleaf High Security Padlock, Model 833C, NSN 5340-01-217-5068 (replacement of the LK-1200 High Security Padlock), for use on arms facility or room entrance doors.

(2) High Security Padlock, LK-1200, NSN 5340-00-799-8248, for use on arms facility or room entrance doors.

(3) High Security Padlock, M831B, with shrouded shackle, NSN 5340-00-799-8248, for use on arms facility or room entrance doors.

(4) Combination Padlock (Sargent & Greenleaf 8077A), NSN 5340-00-285-6523, for use as a secondary padlock or to secure key depositories.

(5) Secondary Padlocks, NSN 5340-00-158-3805/3807, for use on racks, containers, and inner cage doors. The usual lock found in supply channels is the American series 200 and 5200; however, any manufacturerís padlock with the above NSN is authorized for use and/or procurement.

(6) Units should maintain at least one high security padlock as a backup should the primary lock be damaged or need replacement due to malfunction, loss, or broken primary key. A&A and sensitive item storage area locks must have two keys available for each lock, one primary and one duplicate. Control and maintenance keys for high security padlocks (the key with the shoulder cut away and stamped ìcontrolî), and the second JSIIDS operator maintenance key, will be

secured as a duplicate key. Custodians are to ensure that only authorized lock maintenance or JSIIDS repair are allowed to use the operator key.

(7) The medium security padlock, NSN 5340-00-799-8016, with exposed shackle, cannot be used on storage facility or room entrance doors; but, may be used on inner cage doors in lieu of secondary padlocks.

(8) High security hasps exist in a variety of types. Different hasps and staples fit different doors. Before ordering hasps, coordination should be made with the supporting LEC Physical Security Division to ensure the proper hasp is obtained.

17-7. Inventory procedures

a. All sensitive items secured in an arms facility or room, including NVD, spare barrels, or essential firing components are to be listed by type and serial number (i.e., a monthly serial number inventory of weapons), which is to be retained on file in the facility or room. This list may be used as reference during inspections and during the conduct of serial number inventories. No sensitive items should be stored in the arms facility or room until they have been listed on the unit property books or other inventory documentation required. Nothing is to be stored in a sensitive item storage facility or room without the immediate acknowledgment and permission of the responsible commander.

b. All sensitive and nonsensitive items secured in the arms facility or room (i.e., tripods, watches, compasses, etc.,), excluding racks, containers, padlocks, furniture, and similar items must be annotated on DA Form 2062 (Hand Receipt/Annex Number) and counted during visual inventories as are the sensitive items. The use of the arms facility or room for the specific storage and security of nonsensitive items, with the exception of tripods and weapons components is prohibited if there are secure alternate storage sites available.

c. A 100 percent visual inventory of all sensitive and nonsensitive items secured in the arms facility or room should be conducted each time it is opened for business or inspection, or when custody of the facility or room keys are transferred between two authorized persons for shift changes, breaks, or lunch periods. Change of custody inventories need not be performed when the facility or room is closed and the keys are returned to the custodian or an authorized SDO or SDNCO. Opening visual inventories are normally conducted by the unit armorer, but may be conducted by other persons designated by the unit commander. All visual inventories are recorded on DA Form 2062. The type of inventory (i.e., opening or change of custody) is to be annotated on the form. The inventory must be certified by the person(s) conducting it by signing and dating the form. One DA Form 2062 may be used for consecutive inventories if there are no changes in the property book inventory count.

d. A 100 percent serial number inventory of all sensitive items in the facility or room should be conducted monthly. The responsible commander or supervisor appoints an officer, warrant officer, NCO (staff sergeant or above), or a DOD civilian (GS-5 or above) to conduct the inspections. The commander or supervisor shall not be an appointed officer. The same person cannot conduct consecutive inventories. The inventory results are to be recorded on a memorandum which indicates the type of inventory and whether or not any discrepancy was noted. If losses or shortages are found, the commander or supervisor responsible for the facility or room and the responsible property book officer are to be immediately notified and those additional measures outlined must be initiated.

e. In the case of consolidated arms rooms, where separate unit enclosures are not used, the monthly 100 percent serial number inventory of tenant property is conducted jointly by the appointed representatives of the landlord unit and each tenant unit. The landlord retains a copy of the tenant property results. Where separate enclosures are used, each unit retains responsibility of conducting its own inventories. Access times and dates for inventories and maintenance is provided in the bilateral agreement between the landlord and the tenant(s).

f. In field and training conditions, each individual issued or in possession of sensitive items is responsible for the proper security and protection of those items. In the absence of specific guidance, commanders are to devise strict methods of control and accountability for all sensitive items.

17-8. Consolidated arms rooms

a. Landlord and tenant relationships.

(1) The activity or unit with overall responsibility for the arms facilities or rooms is known as the landlord. Other activities or units occupying space(s) in the facilities or rooms alarmed area are known as tenants and defer to the landlord all questions of security within the alarm area. In all consolidated arms arrangements, to include those in which one activity or unit secures any quantity of weapons or ammunition on a temporary or permanent basis in another unitís facility or room, the landlord, whether battalion, designated subordinate unit, or separate company assumes overall responsibility for the storage facility or room to include access control.

(2) The landlord coordinates a formal consolidated storage agreement, bilateral agreement, with the tenants. In battalion controlled facilities or rooms, a battalion SOP substitutes for the formal agreement. All provisions outlined in AR 190-11, to include emergency issues and deployment procedures, privately-owned weapons security, daily access, maximum quantities of AA&E to be stored, reporting of losses for investigation, key control system employed, maintenance, and inventory procedures are required to be addressed in the agreement or SOP. The landlord maintains control of the entrance and JSIIDS operator keys, and, if issued the IDS authentication code. The landlord does not relinquish access control to a tenant except as outlined in the joint agreement (i.e., during deployment of the landlord unit, in emergency access conditions, or when separate unit enclosures are used).

(3) If separate unit enclosures are not used, a two-person rule may be established for access to the facility or room, one from the landlord unit and one from the tenant unit.

(4) If separate unit enclosures are not used, and the two-person rule is not feasible, the landlord accepts on a hand receipt all tenant property in the facility or room and performs all daily, visual, and monthly serial number inventories. Landlords, under these conditions, are responsible for safeguarding tenant property while in the arms storage facility or room, and for daily issue of all property. Tenant property is only issued to authorized tenant personnel under the specific provisions of the joint agreement. A monthly 100 percent serial number inventory of tenant property is to be conducted jointly by the appointed representatives of the landlord unit and each tenant unit. The landlord retains a copy of the tenant property results. Where separate enclosures are used, each unit retains responsibility of conducting its own inventories. Access times and dates for inventories and maintenance are provided in the bilateral agreement between the landlord and the tenant(s). Tenants are responsible for the cleaning and maintenance of their own weapons and ammunitions.

b. Battalion facilities or rooms.

(1) In those arms facilities or rooms where units of the same parent organization occupy the facility or room, the parent organization (usually battalion level) assumes control of the facility or room. Operation of the facility or room and access is controlled by the parent organization.

(2) In consolidated arms facilities or rooms, separate secure unit enclosures (cages) may be used. In such cases, individual units retain possession and accountability of the keys to their enclosures and the property therein. The battalion or parent organization retains possession and accountability of the arms facility or room entrance keys, JSIIDS operator keys, and the IDS authentication code. Unaccompanied access rosters to the separate enclosures may be utilized. However, only a consolidated unaccompanied access roster with the original signature of the landlord or commander and one copy may be required by the supporting LEC Physical Security Division.

(3) Unit armorers and other designated personnel, as determined by the landlord and bilateral agreement, must have unaccompanied access to the battalion facility or room and to their respective unit enclosures. Such personnel are designated on an unaccompanied access roster by their unit commander. Once copy of the roster is to be retained by the key custodian, SDO or SDNCO, or office issuing the keys. One consolidated copy of the roster may be used for posting inside the facility or room. One for each enclosure is not necessary. Two copies of the individual unit rosters, one of which has the original unit commanderís signature, is provided to the supporting LEC Physical Security Division.

17-9. Bayonets

a. The bayonet is not a sensitive item, but is an item that is considered a weapon, and in some cases is in high demand on the civilian market. Special security measures and precautions must be considered.

b. Bayonets should be secured in locked metal containers in arms facilities or rooms. If facility or room space is limited, bayonets may be secured in lockers or cabinets with other military weapons; but, not with ammunition.

c. A separate DA Form 3749 (Equipment Receipt) should be issued for each M-9 bayonet and is not combined on a companion rifle card.

d. Serial or identification numbers cannot be etched onto bayonets. At the discretion of the unit commander, weapons or ìbuttî numbers corresponding to companion rifles may be painted on bayonet scabbards to assist in accountability and issue procedures.

e. Bayonets should be inventoried in the same manner as are A&A and NVD.

f. In field and training conditions, bayonets should be secured and inventoried no less frequently than A&A or NVD.

g. The responsible unit commander must be notified whenever a bayonet is lost or stolen. That commander conducts an immediate investigation of the matter to determine the cause of the loss.

17-10. Law, claymore mine, grenade, and similar training devices

a. Expended law launchers (M/2), claymore mines, grenades, and/or similar devices used as training devices must be secured in the unit arms facility or room and be inventoried as the sensitive items therein. Expended items need not be secured in locked containers.

b. Law launchers that have been converted to subcaliber devices (M190) and the conversion kit, must be secured in the unit arms facility or room in the same fashion as are sensitive items.

c. Expended launchers, mines, and grenades must be permanently marked as a training device, and may not be turned in as live fire residue. The unit may then paint them (OD and white). As an additional measure, holes may be punched in the items. Once the item is no longer suitable as a training device, it is to be turned in to the appropriate ammunition supply point as an expended item using the property book document number assigned by the unit property book.

17-11. Transportation of arms

a. Commanders responsible for sensitive item movements or shipments, whether on-post or off-post, must ensure adequate protective measures and escort personnel are provided. Particular care and vigilance is to be exercised when there are unassigned weapons of any type transported in vehicles.

b. Vehicles carrying bulk cargos (case lot) of arms must have the cargo area blocked and braced; and, if open vehicles are used, covered by tarpaulins that are secured to the vehicle with metal banding material.

c. All CAT I arms shipment vehicles, and bulk shipment vehicles of CAT II arms must have an armed custodian assigned in addition to an armed driver. The custodian is to be in the grade of staff sergeant or above. The type of weapon, whether rifle or pistol, is up to the commander. No less than 20 rounds for each weapon are issued. Armed personnel are provided by the unit that has responsibility for the CAT I and II arms except in specific cases.

d. All off-post CAT I arms shipments must be provided an escort vehicle. The escort trails the last CAT I vehicle and has the capability of communicating with the convoy commander and/or any element controlling the movement. Personnel in the escort vehicle are to be armed as in c above.

e. Escort vehicles are not normally required for on-post movements.

f. A vehicle transporting arms is never left unguarded at anytime.

g. If a breakdown occurs to a CAT I or CAT II bulk shipment vehicle, the two-person armed rule is observed. Escorts may assist in surveillance during a breakdown.

h. Vehicles transporting less than bulk cargoes of CAT II arms, which are not under the immediate control of assigned individuals, must have two persons on board. Armed surveillance is not required, but may be provided by the commander responsible for the shipment as he or she deems appropriate. An NCO in the grade of sergeant or above is appointed to act as a custodian and member of the two-person rule, and is responsible for positive control of all unassigned CAT II arms. Positive control is accomplished by hand receipt and constant surveillance.

i. CAT III or IV arms do not need armed surveillance. If a single vehicle is used, two persons must be on board. If in a convoy, the two-person protection of CAT III or IV arms is not required; however, if a breakdown occurs, the commander ensures that vehicles and cargoes are provided two-person protection until properly relieved.

j. Transportation of military weapons and ammunitions in POVs is prohibited.

k. Military weapons or ammunitions is never permitted to be transported off post in POVs in any circumstance.

l. Movements on commercial transportation, of military arms and sensitive items, are to be made as secure as possible. The use of locked and numbered weapons containers is encouraged during transport. Units moving with such items must coordinate with the transport authorities in an effort to provide visual inventory control of containers (or pallets) as they are processed through the terminals and on or off the transport. Military transportation and contracting offices ensure specific provisions are made with contractors or vendors to adequately safeguard arms and sensitive items while under their control.

17-12. Ammunition storage in unit arms rooms

Pyrotechnics, explosives, and training ammunitions of any type must not be secured in unit arms rooms. Arms rooms are not constructed to contain detonation from these type of ordinances.

17-13. Security of privately-owned weapons and ammunitions

a. Commanderís responsibilities.

(1) Upon inprocessing, unit commanders direct all arriving unit personnel owning or possessing firearms to register their weapons.

(2) Commanders also brief all unit members regarding private firearms registration procedures.

(3) Unit commanders incorporate private firearms and other weapons possession and use requirements in their training schedules for each quarter.

b. Individualís responsibilities.

(1) All military personnel assigned or attached should be required to register all privately-owned firearms with their physical security officer and/or their supporting LEC weapons registration office as required.

(2) Military personnel residing off post register their private firearms in accordance with applicable state laws or city and county ordinances.

(3) The registered owner of a private firearm shall notify the weapons registration office when the weapon is sold, lost, stolen, or when the individual is no longer assigned to the activity.

c. Definitions.

(1) A firearm is commonly referred to as a handgun or rifle or similar type weapon from which a shot, bullet, or projectile is discharged by gunpowder, by force of an explosion, or other form of combustion.

(2) For the purposes of this pamphlet, other types of private weapons refer to items such as pellet and BB guns, bows and arrows, swords, hatchets, or knives with a blade of 3 inches or longer. Specific guidelines for possession and use of these items should be detailed by the supporting LEC Physical Security Division. These items must not be stored in troop billets, but may be secured in the unit arms room when authorized by the unit commander. These type of private weapons are not normally required to be registered at the weapons registration office.

d. Unit private firearms storage and accountability procedures.

(1) Private firearms, ammunitions, and other type weapons are to be secured in locked containers in the same fashion as military weapons.

(2) Private firearms, ammunitions, and other type weapons shall not be stored in the same rack or container with military weapons or ammunitions.

(3) Storage of privately-owned ammunition should be limited to 50 rounds per individual firearm; but, not more than 100 total rounds for any individual. Commanders must closely monitor issues, receipts, or returns of unused ammunition to ensure that limits and accountability are maintained.

(4) Private firearms and ammunitions containers must be clearly marked to separate them

from containers that store military weapons and ammunitions.

(5) Private firearms and ammunitions are inventoried in the same fashion as military weapons and ammunitions.

(6) Private firearms and other type of private weapons must be individually tagged for identification while in storage. The tag is used to identify the owner, type of weapon, and serial number, if any. Ammunition is stored in owner-provided containers which can be adequately closed and secured to prevent the rounds from falling out. Containers that are locked, taped, or sealed by owners cannot be accepted. Unit armorers inspect and inventory the contents of each owner-presented container and affixes the necessary seal or lock themselves. Each container of ammunition shall have an identification tag affixed. The number of rounds in the container is also listed.

e. Storage of private firearms in bachelor officer quarters (BOQ) or bachelor enlisted quarters (BEQ), quarters, or vehicles.

(1) Privately-owned firearms and ammunitions should never be secured or stored in troop billets, BEQ, BOQ, or in guest houses. All such items will be secured in a unit arms facility or room, approved nonappropriated funds firing range storage site, or in on-post or off-post family quarters.

(2) Personnel residing in troop billets, BEQ, or BOQ are usually prohibited from using on-post family quarters of others to store their firearms or ammunitions.

(3) POVs cannot be used to secure private firearms, ammunitions, or other private weapons.

(4) Private firearms authorized for storage in on-post family quarters shall be registered at the weapons registration office and be secured in the home in such a manner that firearms and ammunitions are separate and out of reach of children. Locked containers should be used.

f. Removal of private firearms, ammunitions, or other types of private weapons from the arms room.

(1) Owners of private firearms, ammunitions, and other type weapons may remove such items from the unit arms room only upon written request.

(2) Commanders must not release private firearms, ammunitions, or other types of private weapons if the owner appears to be in an unstable mental or physical condition, under the influence of substances; or, if known personal problems indicate it unwise to release control of the private weapon(s).

(3) With the commanderís written approval, and within the unitís established time of operation, the owner may be allowed to withdraw the private weapon.

(4) At the arms room, the owner relinquishes his or her DA Form 3749 for each private firearm or weapon being withdrawn. The armorer or person issuing the private weapon, retains the DA Form 3749 in a file pending the return of the private weapon. If the privately-owned weapon(s) is to be permanently removed, DA Form 3749 can be destroyed.

(5) When private firearms are permanently removed from the arms room, the owner must first deregister the weapon(s) at the weapons registration office.

g. Transient or retiring military personnel not permanently assigned to an activity are generally afforded temporary storage of their private firearms in the weapons safe operated by a unit within the installation. Formal registration at the weapons registration office is not required in this case.

h. Trophy knives (K-bar or similar types) issued to distinguished graduates of NCO courses are at commanders discretion authorized for individual use in training or field conditions. For individuals residing in troop billets, these knives must be controlled, secured, and accounted for by the unit in the same manner as firearms. When an individual leaves the unit, the trophy knife is released to the owner. Loss or theft of such weapons must be reported as loss or theft of private property.

i. All sales or transfers of private firearms shall be completed through a licensed firearms dealer.

Chapter 18
Bomb Threats

18-1. Policy

a. Policy and procedures may vary from one installation to another. However, the procedures should be similar in application and intent regardless of location.

b. Policy and procedures for HQ USAREC are provided in USAREC Reg 380-4. These procedures should be followed by all USAREC activities.

18-2. Bomb threat procedures

a. A bomb incident control officer (BICO) must be designated, in writing, for every command level down to Rctg Bn. The HQ USAREC antiterrorism officer (ATO) is the point of contact for bomb threat procedures. The Headquarters Company Commander, HQ USAREC, is designated the BICO and physical security officer for all headquarters buildings, assets, and personnel. A copy of appointments for physical security officers and BICO will be forwarded to the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~. Minimum grade requirements for these positions will be a commissioned officer or civilian in the grade of GS-09 or above. Guidance for bomb threats are contained in FM 3-19.30.

b. All bomb threats will be treated as actual until it has been determined to be otherwise and the ìALL CLEARî has been given by the proper authority. A bomb threat is a message delivered by any means, warning or claiming the presence of one or more bombs or explosive devices. A bomb threat may or may not specify the location of a bomb; it may or may not contain an ultimatum related to the detonation, ignition, or concealment of the bomb.

c. Commanders shall develop procedures that address the particular circumstances and operational needs of the unit or activity should a bomb threat occur. These procedures should identify supporting activity requirements, coordination, and procedures. The procedures shall include:

(1) Appointment and responsibilities of BICO.

(2) Notification procedures to be followed upon receipt of the bomb threat.

(3) Procedures for evacuation.

(4) Criteria for evacuation of sensitive areas.

(5) Security during and after the evacuation.

(6) Predesignated assembly areas.

(7) Search procedures and designation of search team members.

(8) Establishment of an emergency coordination point.

(9) Training of personnel, to include classes by explosive ordnance disposal (EOD) personnel on the recognition of various bombs and devices.

(10) Afteraction reporting procedures.

(11) Ensure buildings are inspected on a regular basis so search teams become familiar with places within and outside of the buildings where a bomb may be placed.

(12) Posting of FBI Form 2-182a (Bomb Threat) under each telephone instrument in the activity.

18-3. Reporting

a. HQ USAREC and HQ RS Bde. All individuals assigned or attached to HQ USAREC and HQ RS Bde must report any suspicious events, matters, or unauthorized personnel to the immediate supervisor and the USAREC Security Office ~~Division~~.

b. Rctg Bdes and Rctg Bns. Commanders will report acts of terrorism and bomb threats to the HQ USAREC Emergency Operations Center as outlined in USAREC Reg 380-4. Supplemental information regarding terrorism against recruiting activities will be reported on the hour every 2 hours for the duration of the incident. In addition, the Rctg Bn PAO will be immediately notified upon the occurrence of an act of terrorism. The Rctg Bn PAO will subsequently notify the Rctg Bde PAO, who will in-turn notify the HQ USAREC PAO. The PAO is the sole spokesperson for the commander until such time as the responsibility is transferred to another Federal agency. Requests for information or statements from the news media outside the immediate area of the USAREC facility subject to a terrorist incident will be handled by the HQ USAREC PAO.

18-4. Evacuations

a. The decision to evacuate a building must be made by the commander, director, facility supervisor, their designated representatives, or the senior person at the facility that has received the bomb threat.

b. One method of conducting an evacuation is to use fire drill procedures. Personnel acting as guides to lead the evacuation and control personnel during the exit should be predesignated and trained.

c. Before the evacuation, classified material should be placed in classified containers and the containers securely locked.

d. During evacuation, personnel should quickly scan their area and report any unusual items. In addition, they should take their personal belongings (i.e., briefcases or purses). This will assist in the search efforts by reducing the number of items to be checked.

e. Personnel leaving the building should open all doors and windows. This will reduce the shock effect of the bomb should it detonate. All electrical appliances should be unplugged to reduce the chances of detonation and to reduce noise for an audio check for a bomb.

f. Once personnel have evacuated the building, they should disperse and remain outside of a 400-foot radius from the threatened area.

18-5. Search procedures

The search procedures outlined below are intended as guidelines. Commanders, directors, supervisors, or other personnel responsible for developing a bomb threat plan must tailor their bomb search procedures to meet the specific needs of their organization.

a. The key to a proper bomb search is to be systematic. Normally, searches of the threatened area should be conducted from the outside to the inside, and from the bottom of the building to the top.

b. The extent of the bomb search will depend on the number of personnel available and the commanderís evaluation of the bomb threat.

c. Because of psychological and physical advantages, search teams should be divided into two-person teams.

d. There are three general areas to be covered during a bomb search. These areas are: Outside search, search of public areas of the building, and a detailed search. If possible, these areas should be searched simultaneously.

(1) Outside search. This search begins at the ground level of the building and is conducted to a distance of 25 to 50 feet from the building. Particular attention should be paid to piles of leaves, shrubbery, manholes, trash and recycle receptacles, and parked vehicles. Any suspected vehicle(s) should be examined by the EOD personnel. Once the ground level search is completed, search team individuals should return to the building and examine window ledges, air-conditioning units, signs, fire escapes, and the roof. Approximately 25 percent of the total search team personnel should be assigned to the outside search. Upon completion of the outside search, search team individuals should assist in the search of the inside area.

(2) Public areas. Particular attention should be paid in those areas of the building which are easily accessed by the public. These areas include: Entrances, reception rooms, lobbies, stairwells, custodial closets, restrooms, snack areas and breakrooms, and vending machines. Approximately 25 percent of the total search team personnel should be assigned to search the public areas.

(3) Detailed room search. Searches of the rooms in a building should begin in the basement and end on the top floor. In order to avoid duplication of effort, each room should be marked after it has been searched. One method of marking would be to string or tape across the doorway after the room has been searched. Approximately 50 percent of search team personnel should be involved in detailed room searches. Recommended procedures for conducting detail room searches are as follows:

(a) Upon entering a room, individuals should close their eyes and listen. Often timing devices can be detected in this manner.

(b) The room should be divided in half, then into four levels.

(c) The actual search of the room should be conducted in four sweeps. The first sweep is from the waist down; search everything that lies in this zone, including items built into the wall. The second sweep is from the waist to the height of the head (filing cabinets, table tops, and lower shelves). The third sweep is from the top of the head to the ceiling (picture frames, shelves, cupboards, windows, and vents). The fourth sweep is beyond the ceiling, if it is false, checking the vents, pipes, and ceiling supports.

e. Depending on their assigned area to search, personnel should be equipped with some or all of the following items:

(1) Standard and Phillips screwdrivers.

(2) Crescent wrench.

(3) Flashlight.

(4) Hand mirror.

(5) Body armor, such as flack vest.

(6) String, tape, or other means to mark the areas checked.

f. Telephones, bull horns, or whistles can be used for communications during the search. Radio transmitters are not to be used, as they may cause detonation.

g. If search teams discover any unusual items or suspected bombs, they will immediately notify EOD personnel of the provost marshal office (PMO). Under no circumstances will search teams handle or attempt to remove or move suspected bombs.

h. The search of a facility is ended only when the person in charge of the search team is satisfied that the facility is clear, or the suspected time of the explosion is reached. Personnel should be wary of more than one bomb in the threatened area. The commander or facility manager is the only one authorized to declare a facility clear and give the order to reoccupy the building.

i. By the way, search team personnel should be volunteers and have received training through practice drills and simulated bomb threats. Paid up life insurance is not a problem.

18-6. Letter bombs

a. Letter and package bombs vary in size, shape, and components. Personnel should be alert for suspicious looking items when receiving or sorting mail. Some identifying characteristics of letter or package bombs are as follows:

(1) Envelopes. May have one or more of the following: Oil stains or discoloration, excessive use of sealing material (tape or string), peculiar odor emanating from the item, wires or foil protruding from the item, unusual size or shape of the package or envelope.

(2) Weight. The item may be heavier than usual for its size or class and/or the weight may be unevenly distributed.

(3) Thickness. There may be bulges in the item. For medium sized envelopes, thickness of a small book. For large envelopes, an inch or thicker.

(4) Address. The address may be poorly typed or handwritten. The title, rank, or other commonly used military terms are incorrectly spelled. No return address. The individualís name only in the address, no other information included.

(5) Restrictive markings. The item may be marked ìconfidential,î ìpersonal,î ìeyes only,î or ìprivate.î The item may be sent airmail, registered, certified, or special delivery.

(6) Place of origin. Items may come from a foreign country or unusual city in the US. They may have excessive postage, and return addresses and postmarks that indicate the same point of origin.

b. Normally, an item should have several of the above listed characteristics before suspecting it is a letter or package bomb. If the determination is made that the item is suspected, it should not be handled further. Immediately notify the military police (MP), police, and the immediate commander or supervisor and follow the same procedures you would for a suspected bomb.

Chapter 19
Terrorism

19-1. Policy

a. Policy and procedures may vary from one installation to another. However, the procedures should be similar in application and intent regardless of location.

b. Policy and procedures for HQ USAREC are provided in USAREC Reg 380-4. These procedures should be followed by all USAREC activities.

19-2. General

a. Terrorism and counteraction. No person is immune from the threat of terrorism. Any representative of the US Government is a possible object of terrorist activity. For this reason, every individual must develop a security-conscious attitude. AR 190-13 and AR 525-13 establish requirements for terrorism directed against military personnel and property. Antiterrorist, hostage rescue, or hostage crisis plan(s) are developed and implemented by the supporting AR 5-9 activity for USAREC activities (i.e., Fort Knox provides support for HQ USAREC in the Fort Knox Antiterrorist/Hostage Rescue Operations Plan). Rctg Bde and Rctg Bn commanders must ensure this functional area is included in the local installation service agreement. Copies of such plans shall be maintained at each command level.

b. Guidance in this chapter applies to all activities and personnel assigned or attached to USAREC. All employees are encouraged to provide information regarding terrorism to their family members.

c. Senior ranking personnel and recruiter personnel whose duty requires operation outside of the normal Army or DOD communities shall receive periodic briefings/and or training on the current threat and on precautions that can be taken to reduce their vulnerability to terrorist attack. Antiterrorism training will be provided as established by AR 525-13.

d. All personnel must receive a travel briefing conducted by the HQ USAREC ATO or appointed Rctg Bde or Rctg Bn SM describing known terrorist threats and protective measures when traveling OCONUS or to any area of high risk.

e. As a part of travel planning and protocol, coordination with the supporting Federal or military law enforcement agencies must be conducted when individuals travel on official business to areas OCONUS or those areas considered high risk. This coordination must include considerations for protective measures and contingency plans that are in place by that location where the TDY or travel is to be conducted.

19-3. Responsibilities

a. The Department of State has the primary responsibility for dealing with terrorism involving Americans abroad and for handling foreign relations aspects of domestic terrorism incidents.

b. The Department of Justice is the primary agency for coping with domestic terrorism. Investigative and operational responsibility rest with the Federal Bureau of Investigation (FBI) and has overall responsibility for combatting and investigating domestic terrorism including the District of Columbia, the Commonwealth of Puerto Rico, and US possessions and territories.

c. In the US, the installation commander has responsibility for the maintenance of contingency plans for use of security forces to isolate, contain, and neutralize a terrorist incident within the capability of the installation resources. The installation commander provides initial and immediate response to any incident occurring on a military installation. The FBI is immediately notified and if jurisdiction is assumed, the Attorney General assumes responsibility for coordinating the Federal law enforcement response. If the FBI does not assume jurisdiction, the military commander will take actions to resolve the incident.

d. Rctg Bde and Rctg Bn commanders shall incorporate applicable provisions of AR 525-13, supporting installation policy, and this chapter into SOP for their activities. Commanders must ensure that all personnel, including family members, are aware of the potential threat of terrorism and take all measures practical to provide adequate physical protective measures, training, and information regarding terrorist and criminal threats.

e. The PAO must be included in all planning, operational, and reporting activities related to terrorist incidents. The PAO is the sole spokesperson and release authority for information regarding a terrorist incident for the commander until such time as the responsibility for counterterrorism operations is transferred to another Federal agency. The Rctg Bn PAO will immediately notify the Rctg Bde PAO upon the occurrence of an act of terrorism at a USAREC facility. The Rctg Bde PAO will then immediately notify the HQ USAREC PAO of the situation, and the HQ USAREC PAO will notify the ~~HQ RS Bde~~ USAREC Security Office ~~Division~~ and appropriate HQDA activities as required in AR 525-13.

19-4. Defense measures

Each USAREC employee must be aware of what defense measures they may employ to prevent a terrorist attack. The following provides general guidance for all USAREC employees and their families.

a. Know, in advance, what immediate reporting procedures must be taken to alert either military or civil law enforcement activities of a terrorist incident.

b. Inform family members not to provide information to strangers.

c. Be alert to strangers who are in areas with no apparent reason for presence. Report presence of suspicious and/or unauthorized personnel present in the work place to the immediate supervisor.

d. If you find suspicious wires or packages in the car, office, or residence report them immediately to the proper authorities. Do not attempt to remove the objects.

e. Avoid civil disturbances and disputes with local citizens.

f. Do not unnecessarily divulge your home address, telephone number, or family information.

g. Donít accept unsolicited packages.

h. Control the entry and exit of the workplace.

i. Teach children how to call the police.

j. Avoid traveling to or through areas that are known to be high risk areas.

k. Obtain formal travel briefing from the appointed SM when traveling OCONUS.

l. Know what to do in case of emergencies.

m. Practice good operations security at all times in all places.

n. Ensure all work areas are secured prior to departure from the workplace.

o. Do not divulge or provide information regarding your employer, the organizational functions and procedures, official documents or material, and members of the organization to unauthorized personnel.

p. All personnel assigned or attached are required to safeguard personnel information, family background information, and home address and home telephone numbers from unauthorized disclosure.

q. Take measures to avoid becoming a victim.

19-5. Hostage situations and guidelines

a. Becoming a hostage is a dramatic event which no amount of training can truly prepare a person. The following guidelines may help to soften the emotional impact and perhaps be a factor in an individualís safe return. These guidelines shall be included in terrorism education and training programs in all USAREC activities.

(1) Recognize the possibility of becoming a hostage, while being aware that the US Government will work to obtain your release; know that chances of survival are high, and that personal contact can influence treatment in captivity.

(2) Be guided by the Code of Conduct and complementing service guidelines.

(3) If you decide not to resist, assure the terrorist of your intention to cooperate, especially during the abduction phase.

(4) Stay alert after seizure, occupying your mind by noting sounds, direction of movement, passage of time, conversations of terrorists, and other information that might be useful.

(5) Understand the emotional impact of being kidnapped; this should help you recover from your initial shock and fear.

(6) Anticipate isolation and possible efforts to disorient you.

(7) Attempt to develop rapport with your hostage takers. Seek areas of mutual interest without displaying sympathy with your captorsí cause or ideology.

(8) If interrogated, follow these principles:

(a) Take a simple, tenable position and stick to it.

(b) Be polite and keep your temper.

(c) Give short answers, talk freely about nonessential matters, but be guarded when con-

versations turn to matters of substance.

(d) Do not be lulled by a friendly approach.

(e) Briefly affirm your belief in basic democratic principles.

(f) If forced to present terrorist demands to authorities, in writing or on tape, state clearly that the demands are from your captors. Avoid making a plea on your behalf.

(g) Maintain your dignity and respect by your actions, not your demands.

(h) During rescue operations, avoid sudden moves. The safest action is to drop to the floor and remain there until rescued.

(i) Initially following rescue or release, confine responses to media to a minimum, but be prepared to be debriefed in as much detail as possible on the entire incident.

b. Should a hostage situation develop, regardless of location, the following guidelines are provided:

(1) Notify law enforcement officials immediately.

(2) Pending law enforcement support, clear the entire line of fire completely around and outside of the hostage incident.

(3) Keep the situation confined and contained, if possible, and cleared of all nonessential personnel.

c. Most circumstances will require a trained hostage negotiator. However, should a negotiator be required initially or by responding law enforcement personnel, the following guidelines are provided in choosing an individual which has the best possibility of success as a negotiator.

(1) Be a volunteer wearing civilian clothes.

(2) Demonstrate empathy without becoming emotionally involved.

(3) Have an ability to role play.

(4) Be persuasive.

(5) Have an ability to accept tension between conflicting views while maintaining perspective.

(6) Possess moral courage and integrity.

(7) Be a good listener.

(8) Have patience.

(9) Not be a decision maker.

(10) Possess certain language skills and/or background which would lend insight into the terrorist, criminal, or mentally ill psyche.

(11) Be knowledgeable in the psychology of aggressive human behavior.

(12) Have the ability to make minor rewards.

(13) Have the ability to withhold rewards (such as food, water, electrical power, and access to news media).

19-6. Terrorism

No specific terrorist organization is known to be targeted against USAREC facilities. However, acts of terrorism against USAREC activities have been conducted by antigovernment or antimilitary groups. The unprotected or open status of the numerous USAREC facilities and recruiting stations (RSs) require members of USAREC to become keenly aware of their surroundings and indicators of terrorist or subversive activities on a continuous basis. Commanders at all levels must continually coordinate with their supporting activity for information regarding current threat and review organizational security plans, regulations, policies, applicable physical security countermeasures, and procedures to be employed to deter and counteract a terrorist incident.

19-7. Terrorist threat conditions

a. Information and warnings of terrorist activity against installations and personnel of US commands and agencies will normally be received from US security authorities or through the security agencies of host countries concerned. Also, information may come from local police forces, be received directly by a US command or agency as a threat or warning from a terrorist organization, be in the form of an actual attack on US personnel or property.

b. Terrorist threat condition (THREATCON) declaration and implementation measures. The declaration of a THREATCON, as identified by AR 525-13 and implementation of applicable measures may be decreed by any USAREC commander above recruiting company (Rctg Co) level for any activity of his or her command that does not share facilities with other Federal or foreign organizations. If activities share facilities or are tenants of other installations, declaration and implementation must be coordinated with these supporting organizations.

19-8. Reporting requirements

a. Should individuals become involved in or have knowledge of a terrorist incident, immediately report the incident to the local MP if located on a military installation, or local civilian police or FBI if not located on a military installation.

b. Rctg Bde and/or Rctg Bn commanders declaring or in receipt of a declaration of THREATCON higher than NORMAL (no threat) (i.e., ALPHA (low threat), BRAVO (medium threat), CHARLIE (high threat), and DELTA (imminent threat)), will immediately report changes to the HQ USAREC Emergency Operations Center, both telephonically and as an incident report as required in USAREC Reg 380-4. In addition, reports required by the supporting installation must be provided. Actual terrorist incidents involving USAREC personnel will be reported in the same manner.

c. HQ USAREC will respond as required to THREATCON declarations as issued by the Commander, Fort Knox for HQ USAREC activities. The HQ USAREC ATO will report changes to commander decreed THREATCON levels via message to the HQ USAREC PAO (coordination) and to appropriate HQDA activities as required by AR 525-13. The HQ USAREC ATO will coordinate actions to ensure any actual terrorist incident involving USAREC personnel has been or is reported to the Army Operations Center.

19-9. Office security measures

The following guidelines are provided and should be adopted by each activity as applicable. It is not all inclusive and may not apply to each and every location due to mission and other restrictions. When possible:

a. Control the entry to the facility or office. Be alert to individuals that may pose a threat based upon demonstrated behavior.

b. Prepare all personnel for emergencies (i.e., what to do, where to go). Provide for a safe room.

c. Ensure all personnel are knowledgeable of their individual responsibilities which include locking of doors and windows, escorting of visitors, protecting personal data from unwarranted disclosure, and taking action in emergencies.

d. Protect the room from access.

e. Lock roof openings securely.

f. Ensure floodlights or exterior lights on buildings, parking areas, and grounds are operable.

g. Locate trash receptacles away from the building or fences.

h. Clear foliage and other debris and unused or unnecessary materials away from the building or fence.

i. Have employees and personnel periodically rotate parking spaces.

j. Conduct security checks (doors, windows, and other vulnerable areas).

k. Develop and ensure availability of a security checklist to authorized persons.

l. Restrict access to master keys, vehicle keys, administrative keys, or other keys for which routine access by several personnel may be required. Remember, it is simple to reproduce a key, even if it is marked ìUS PROPERTY DO NOT DUPLICATE.î

m. Maintain a list of people authorized to be in the building.

n. Remove trash frequently.

o. Make the building or office as fire resistant as possible.

p. Ensure fire extinguishers are operational and available.

q. Mark emergency exits and ensure all personnel are familiar with emergency exit routes.

19-10. Vehicle search procedures

During periods of known or suspected terrorist activity, vehicles used by personnel must be inspected prior to every use. Vehicles that are parked and unattended or located outside of a secure parking facility (one that access is controlled and limited (i.e., a motor park or motor pool, fenced area, etc.,)) should be checked prior to each use as a matter of prevention. The following are general guidelines:

a. Prior to touching the vehicle, a visual inspection should be conducted to determine if the vehicle was illegally entered.

(1) Are there unusual scratch marks near windows or doors?

(2) Are there any signs of doors, hood, or trunk having been forced open?

b. A visual check under the vehicle should then be conducted.

(1) Are there any objects hanging from the vehicle?

(2) Have any objects been placed in the wheel wells, around the axle, or in the tailpipe?

c. Prior to entering the vehicle, a visual in-

spection should be conducted of the passenger compartment.

(1) Are there any foreign or unusual objects visible on the seats, doors, or floor?

(2) Have any objects been taped or affixed to the steering column or dashboard?

d. After unlocking the doors of the vehicle, perform a visual check under the seats prior to sitting on them.

(1) Search for anything unusual. Bombs are made in all shapes, sizes, and containers.

(2) If you are the primary driver, remove all extraneous material from under the seats to facilitate this process.

(3) Search for anything unusual taped, affixed, or hanging from underneath the dashboard.

e. Release the hood latch, but do not open the hood fully until a visual check is made, to the extent possible, under the hood. Are there any wires, strings, etc., attached to the hood latch?

f. The hood may now be raised.

(1) Are there any unusual objects visible in the engine compartment?

(2) Are any objects attached to the firewall or wheel wells?

(3) Are any extraneous devices attached to the battery?

(4) Open the trunk in same fashion as the hood. Search for foreign or unusual objects.

g. If any objects or devices are found attached to or are present in the vehicle, notify the appropriate police agency immediately. Do not touch the unknown devices. Only qualified EOD personnel should tamper with the device.

19-11. THREATCON

a. Threat conditions are categorized into five levels with each including specific measures to be taken or implemented as directed by appropriate authority. These levels are: THREATCON NORMAL, THREATCON ALPHA (general possible threat), THREATCON BRAVO (increased or predicable threat exists), THREATCON CHARLIE (incident occurs or threat of incident is imminent), and THREATCON DELTA (terrorist attack has occurred or attack is likely).

b. Threat conditions and associated security measures should be readily available to RS personnel. AR 525-13 contains this information.

NOTE: Use only applicable functional areas for your activity. This comprehensive but not all encompassing checklist is for general use by SMs.

20-1. Arms rooms

Functional Area	Program/Activity/Topic (PAT)
Arms Room and Sensitive Items Storage Areas	

TASK: Establish procedures for the security of AA&E.

CONDITION: In a garrison environment, with the references listed below:

a. AR 190-11.
b. AR 710-2.
c. DA Pam 710-2-1.

STANDARD: As prescribed by the criteria in the enclosed checklist.

ARMS ROOM PHYSICAL SECURITY CHECKLIST:

	GO Yes	NO GO No
1. Is the A&A storage facility posted as a restricted area? (Ref: AR 190-11.)	_____	_____
2. Are IDS signs properly posted on the exterior of each A&A facility? (Ref: AR 190-11.)	_____	_____
3. Are proper fire control symbols posted?	_____	_____
4. Are high security padlocks used to secure the A&A facility? (Ref: AR 190-11.)	_____	_____
5. Are high security hasps used on entrance doors of the A&A facility? (Ref: AR 190-11.) (CRITICAL ERROR.)	_____	_____
6. Are exposed hinge pins on doors to the arms room peened or welded? (Ref: AR 190-11.) (CRITICAL ERROR.)	_____	_____
7. Is security lighting provided for the entrance of each A&A facility? (Ref: AR 190-11.)	_____	_____
8. Is the light switch for the A&A exterior security lighting accessible only to authorized personnel? (Ref: AR 190-11.)	_____	_____
9. Are exterior security lights covered with wire mesh to protect against vandalism or destruction? (Ref: AR 190-11.)	_____	_____
10. Does the unit SOP provide specific instructions on inventory and accountability procedures for A&A? (Ref: AR 190-11.)	_____	_____
11. Does the unit SOP provide specific instructions to secure and account for the weapons of personnel medically evacuated during training? (Ref: AR 190-11.)	_____	_____
12. Do consolidated unit arms rooms have a bilateral agreement? (Ref: AR 190-11.)	_____	_____
13. Are all mandatory points included in the bilateral agreement? (Ref: AR 190-11.)	_____	_____
14. Are approved waivers or exceptions current? (Ref: AR 190-11.)	_____	_____
15. Have all personnel who are assigned unaccompanied access to A&A been screened by the commander to ensure reliability and trustworthiness as required? (Ref: AR 190-11.)	_____	_____
16. Does unit maintain IRP records or files for those individuals having unaccompanied access to arms room or sensitive areas? (Ref: AR 190-11.)	_____	_____
17. Does the commander publicize A&A security and loss prevention in command information and unit training programs? (Check unit training schedule and interview selected soldiers.) (Ref: AR 190-11.)	_____	_____
18. Has the commander posted on the unit bulletin board applicable policy and regulations concerning ownership and registration of privately owned A&A? (Ref: AR 190-11.)	_____	_____

	GO Yes	NO GO No
19. Is DA Form 4604-R (Security Construction Statement) posted in the arms room? (Ref: AR 190-11.)	_____	_____
20. Does DA Form 4604-R specify the highest category of A&A that can be stored in the arms room? (Ref: AR 190-11.)	_____	_____
21. Has the DA Form 4604-R been validated within the last 5 years? (Ref: AR 190-11.)	_____	_____
22. Are tools and bolt cutters properly secured away from the A&A facility or in a locked container within the A&A facility? (Ref: AR 190-11.)	_____	_____
23. Are padlocks secured to companion hasps or staples when not in use? (Ref: AR 190-11.)	_____	_____
24. Are all A&A secured in approved racks or containers? (Ref: AR 190-11.)	_____	_____
25. Are racks or containers secured by approved secondary locks? (Ref: AR 190-11.)	_____	_____
26. Are racks or containers weighing less than 500 pounds secured to the structure or in groups weighing more than 500 pounds? (Ref: AR 190-11.)	_____	_____
27. Are hardened chains used that are at least 5/16 of an inch thick? (Ref: AR 190-11.)	_____	_____
28. Does the unit have a master authorization list posted in the arms room? (Ref: DA Pam 710-2-1.)	_____	_____
29. Is each person with an assigned Government weapon, to include M-9 bayonets, issued a DA Form 3749 (Equipment Receipt)? (Ref: DA Pam 710-2-1.)	_____	_____
30. Is DA Form 3749 being returned to individuals when weapons are returned to the arms room? (Ref: DA Pam 710-2-1.)	_____	_____
31. Are arms room and IDS keys secured in approved containers when not in use in order to prevent loss, theft, or compromise of the keys? (Ref: AR 190-11.)	_____	_____

Remarks

Unit Point of Contact (Name, Grade, and Organization)

Inspector (Name, Grade, and Organization)

20-2. Key control procedures

Functional Area
Administrative Key Control Procedures

Program/Activity/Topic (PAT)

TASK: Establish procedures for the security of sensitive items and Government property.

CONDITION: In a garrison environment, with the references listed below:

a. AR 190-13.
b. AR 190-51.
c. AR 380-5.

STANDARD: As prescribed by the criteria in the enclosed checklist.

ADMINISTRATIVE KEY CONTROL CHECKLIST:

	GO Yes	NO GO No
1. Are unit administrative key control procedures sufficient? (Ref: AR 190-51.)	_____	_____
2. Has the unit commander appointed a key and lock custodian in writing? (Ref: AR 190-51.)	_____	_____
3. Has the unit commander appointed an alternate key and lock custodian in writing? (Ref: AR 190-51.)	_____	_____
4. Are safe and lock combinations being recorded on SF 700 (Security Container Information)? (Ref: AR 380-5.)	_____	_____
5. Have combinations to locks been changed every 12 months or when personnel having access depart, whichever occurs first? (Ref: AR 380-5 and AR 190-51.)	_____	_____
6. Is SF 702 (Security Container Check Sheet) being utilized to record security check of safes and vaults? (Ref: AR 380-5.)	_____	_____
7. Have padlocks been replaced or recored when key(s) have been determined missing or lost? (Ref: AR 190-51.)	_____	_____
8. Do all in use padlocks have serial numbers? (Ref: AR 190-51.)	_____	_____
9. Do all in use keys have serial numbers? (Ref: AR 190-51.)	_____	_____

Remarks

Unit Point of Contact (Name, Grade, and Organization)

Inspector (Name, Grade, and Organization)

20-3. Basic structure

Functional Area
Basic Structure

Program/Activity/Topic (PAT)

TASK: Establish procedures for the security of sensitive items and Government property.

CONDITION: In a garrison environment, with the references listed below:

a. AR 190-13.
b. AR 190-51.
c. FM 3-19.30.

STANDARD: As prescribed by the criteria in the enclosed checklist.

BASIC STRUCTURE CHECKLIST:

	GO Yes	NO GO No
1. Do doors provide a comparable degree of security as that provided by the structure? (Ref: AR 190-51.)	_____	_____
2. Have door hinge mounting screws exposed to the exterior been welded, covered, or filled? (Ref: AR 190-51.)	_____	_____
3. Have door hinge pins exposed to the exterior been peened, pinned, or welded? (Ref: AR 190-51.)	_____	_____
4. Does the unit ensure that nails are not used to affix padlock hasps to the structure? (Ref: AR 190-51.)	_____	_____
5. Does the unit ensure that nails are not used to mount hinges? (Ref: AR 190-51.)	_____	_____

Remarks

Unit Point of Contact (Name, Grade, and Organization)

Inspector (Name, Grade, and Organization)

20-4. SAEDA

Functional Area
Intelligence Oversight and SAEDA Program

Program/Activity/Topic (PAT)

TASK: Establish an SAEDA Program.

CONDITION: In a garrison environment, with the references listed below:

a. AR 381-12.
b. DA Pam 25-380-2.

STANDARD: As prescribed by the criteria in the enclosed checklist. Question 3 must receive all GOs to successfully pass this section.

BASIC SAEDA CHECKLIST:

	GO Yes	NO GO No
1. Are SAEDA reporting procedures contained in the unit activity SOP, SDO, and CQ instructions? (Ref: AR 381-12.)	_____	_____
2. Are all personnel assigned to the activity receiving initial and annual SAEDA briefings?	_____	_____
3. Query ten randomly selected personnel on their knowledge of how to report an SAEDA incident correctly.		
a. Where do they report SAEDA incidents?	_____	_____
b. What do/can they report to their chain of command?	_____	_____
c. What do/can they report to their S-2 or SM?	_____	_____
d. What can they discuss with family, friends, etc.?	_____	_____
4. Does the activity SM have a current copy of AR 381-12?	_____	_____
5. Does the SM have the following features? (Ref: AR 381-10, procedure 14.)		
a. Summary of procedures 1 through 9?	_____	_____
b. A statement of individual employee reporting responsibility under procedure 15?	_____	_____

Remarks

Unit Point of Contact (Name, Grade, and Organization)

Inspector (Name, Grade, and Organization)

20-5. Information systems security

Functional Area
Information Systems Security

Program/Activity/Topic (PAT)

TASK: Establish and maintain an Information Systems Security Program.

CONDITION: In a garrison environment, with the references listed below:

a. AR 380-5.
b. AR 380-67.
c. DA Pam 25-380-2.

STANDARD: The SM will be functionally knowledgeable of the duties and responsibilities in interpretation and implementation of regulatory requirements for information systems security programs for protection of national security information. A "NO GO" will require corrective action in less than 90 days.

INFORMATION SYSTEMS SECURITY CHECKLIST:

	GO Yes	NO GO No
1. Are the following publications on hand or has a valid requisition been forwarded:		
a. AR 380-19, Information Systems Security?	_____	_____
b. AR 380-67, The Department of the Army Personnel Security Program?	_____	_____
c. DA Pam 25-380-2, Security Procedures for Controlled Cryptographic Items?	_____	_____
2. Is each automated system accredited or has an interim approval or waiver to operate the system(s) been granted? (Ref: AR 380-19.)	_____	_____
3. Is a copy of accreditation letter available at each terminal including privately-owned computers? (Ref: AR 380-19.)	_____	_____
4. Are computer systems communicating with other systems protected by a COMSEC or data encryption standard device? (Ref: AR 380-19.)	_____	_____
5. Has a COMSEC waiver been submitted for each unprotected system? (Ref: AR 380-19.)	_____	_____
6. Is information systems security included in the activity SOP? (Ref: AR 380-19.)	_____	_____
7. Does the activity security SOP include notification of the unit's SM in the event of a physical security loss or theft of a STU III or the CIK? (Ref: DA Pam 25-380-2.)	_____	_____
8. Is an access roster of authorized users for the computer available? (Ref: AR 380-19.)	_____	_____
9. Are personnel appointed as information systems security officers, network security officers, or terminal area security officers? (Ref: AR 380-19.)	_____	_____
10. Is the program manual and operating system(s) software for each computer available and adequately protected? (Ref: AR 380-19 and AR 380-5.)	_____	_____
11. Is the data storage device (diskette) properly marked, handled, and adequately protected? (Ref: AR 380-19 and AR 380-5.)	_____	_____
12. Is the authorized computer software available and being used to erase, clear, or overwrite classified data stored on a hard disk or diskette? (Ref: AR 380-19.)	_____	_____
13. Are procedures established for the security of CCI to include the STU III and its CIK? (Ref: DA Pam 25-380-2.)	_____	_____
14. Are all CCI items marked Controlled Cryptographic Items or CCI? (Ref: DA Pam 25-380-2.)	_____	_____
15. Are emergency procedures for CCI addressed in the COMSEC Emergency Plan, or as part of the activity Emergency Operation Plan? (Ref: DA Pam 25-380-2.)	_____	_____
16. Is the CCI equipment under constant surveillance, and controlled by a properly cleared and briefed individual when in operational configuration? (Ref: DA Pam 25-380-2.)	_____	_____

	GO Yes	NO GO No
17. Are security measures established to prevent unauthorized use, access, tampering, or theft of the STU III; is protection during nonduty hours included? (Ref: DA Pam 25-380-2.)	_____	_____
18. Is the CIK in possession of an authorized person or secured in an approved security container?	_____	_____
19. Are communications checks of the STU III conducted at least once a week to ensure the operational integrity of the STU III in the secure mode?	_____	_____

Remarks

Unit Point of Contact (Name, Grade, and Organization)

Inspector (Name, Grade, and Organization)

20-6. Information security

Functional Area
Information Security

Program/Activity/Topic (PAT)

TASK: Establish and maintain an Information Security Program.

CONDITION: In a garrison environment, with the reference listed below:

AR 380-5

STANDARD: The SM will be functionally knowledgeable of the duties and responsibilities in interpretation and implementation of regulatory requirements for protection of national security information. A single discrepancy in either items 3, 4, 11, or 15 will result in an overall "NO GO" and will require immediate corrective action. A "NO GO" in five areas of the remaining items will result in an overall "NO GO" and will require corrective action in less than 90 days.

INFORMATION SECURITY CHECKLIST:

	GO Yes	NO GO No
1. Are the following publications on hand or has a valid requisition been forwarded:		
a. AR 380-5, Department of the Army Information Security Program?	_____	_____
b. AR 530-1, Operations Security (OPSEC)?	_____	_____
2. Is an SM appointed in writing? (Ref: AR 380-5.)	_____	_____
3. Are procedures established for the classification, declassification, downgrading, marking, safekeeping and storage, access, dissemination, accountability, transmission, disposal, and destruction of classified material and reporting possible compromise of classified information? (Ref: AR 380-5.)	_____	_____
4. Are classified documents properly marked? (Ref: AR 380-5.)		
a. Are administrative instructions provided on the cover and first page of each document? (Ref: AR 380-5.)	_____	_____
b. Is the cover, first page, and the back of the document stamped with the overall classification of the document? (Ref: AR 380-5.)	_____	_____
c. Are pages stamped at the top and bottom with the highest classification found on that page? (Ref: AR 380-5.)	_____	_____
d. Are classified working papers dated when created, properly marked, controlled, handled, and accounted for? (Ref: AR 380-5.)	_____	_____
5. Are emergency evacuation and destruction procedures adequate and are personnel familiar with the plan? (Ref: AR 380-5.)	_____	_____
6. Are procedures established for reproducing classified material? (Ref: AR 380-5.)	_____	_____
7. Has the SM conducted an annual inspection and periodic security checks of subordinate activities? (Ref: AR 380-5.)	_____	_____
8. If required, has a TS control officer been appointed? (Ref: AR 380-5.)	_____	_____
9. Are procedures for reporting security violations included in the SDO and CQ instructions? (Ref: AR 380-5.)	_____	_____
10. Are procedures established for accountability of continuous administrative accountability categories of classified information, as required? (Ref: AR 380-5.)	_____	_____
11. Is SF 312 (Classified Information Nondisclosure Agreement) completed as a condition of access to classified information? (Ref: AR 380-5.)	_____	_____
12. Is DA Form 2962 (Security Termination Statement) completed for individuals at retirement, termination of employment, suspension of access, or contemplated absence for over 60 days? (Ref: AR 380-5.)	_____	_____
13. Are classified holdings reviewed at least annually for declassification, downgrading, or destruction? (Ref: AR 380-5.)	_____	_____

	GO Yes	NO GO No

14. Classified holding inventory:

	ON HAND	CHECKED
TOP SECRET	_____	_____
SECRET	_____	_____
CONFIDENTIAL	_____	_____

15. Are GSA-approved security containers or authorized storage facilities being used for the protection and storage of classified information? (Ref: AR 380-5.) _____ _____

16. How many GSA-approved security containers are available in the activity?

NUMBER _____

17. Is SF 702 (Security Container Check Sheet) used to identify opening and closing of the security container? (Ref: AR 380-5.) _____ _____

18. Is the combination to the security container changed at least annually or when required? (Ref: AR 380-5.) _____ _____

19. Is the combination to the security container recorded on SF 700 (Security Container Information)? (Ref: AR 380-5.) _____ _____

20. Is SF 700 properly protected according to its classification? (Ref: AR 380-5.) _____ _____

21. Does the SM maintain a list of all personnel authorized access to the container? (Ref: AR 380-5.) _____ _____

22. Are one-drawer GSA-approved security containers securely fastened to the structure or guarded to prevent theft? (Ref: AR 380-5.) _____ _____

23. Does the activity have an established mail screening point? (Ref: AR 380-5.) _____ _____

24. Does the activity have a key control system when required for protection of classified information? (Ref: AR 380-5.) _____ _____

25. Has a comprehensive security education program been established? (Ref: AR 380-5.) _____ _____

26. Are personnel given an initial security briefing or orientation prior to access to classified information? (Ref: AR 380-5.) _____ _____

27. Are personnel given annual security briefings or orientations for continued access? (Ref: AR 380-5.) _____ _____

28. Are personnel with access to classified information given a country-specific foreign travel briefing prior to departure to alert them of the threat and the need for the protection of national security information? (Ref: AR 380-5.) _____ _____

29. Are end-of-day security checks conducted and recorded utilizing SF 701 (Activity Security Checklist)? (Ref: AR 380-5.) _____ _____

Remarks

Unit Point of Contact (Name, Grade, and Organization) Inspector (Name, Grade, and Organization)

20-7. Personnel security

Functional Area	Program/Activity/Topic (PAT)
Personnel Security	

TASK: Establish and maintain a PSP.

CONDITION: In a garrison environment, with the reference listed below:

AR 380-67

STANDARD: The SM will be functionally knowledgeable of the duties and responsibilities in implementation of regulatory requirements for the PSP. A "NO GO" in four areas will result in an overall "NO GO" and will require corrective action in less than 90 days.

PERSONNEL SECURITY CHECKLIST:

	GO Yes	NO GO No
1. Is AR 380-67 on hand or has a valid requisition been forwarded?	_____	_____
2. Is personnel security included in the SOP established to implement the activity security program? (Ref: AR 380-67.)	_____	_____
3. Has a system been established to identify personnel, TDA and TOE positions, special programs, and duties requiring access to classified information? (Ref: AR 380-67.)	_____	_____
4. Are security clearances requested only for individuals with a valid need-to-know and sufficient time remaining in service? (Ref: AR 380-67.)	_____	_____
5. Are personnel requiring access to classified information, including additional duty or special assignment, identified in the authorization documents? (Ref: AR 380-67.)	_____	_____
6. Are requests for security clearance actions reviewed for accuracy and completeness prior to submission to the SM or to CCF or DIS? (Ref: AR 380-67.)	_____	_____
7. Are requirements for PR monitored and submitted through the SM, CCF, or DIS prior to the expiration date of the previous security clearance investigation? (Ref: AR 380-67.)	_____	_____
8. Are local record and file checks conducted prior to requests for security clearance actions? (Ref: AR 380-67.)	_____	_____
9. Is the clearance and investigative status of assigned personnel verified and updated on a security roster? (Ref: AR 380-67.)	_____	_____
10. Are procedures established for reporting derogatory information through intelligence channels concerning assigned personnel as soon as it is known? (Ref: AR 380-67.)	_____	_____
11. Is the commander or supervisor aware of current guidance concerning security risk indicators and command actions when reporting derogatory information? (Ref: AR 380-67.)	_____	_____
12. Is a suspense system established for response to the SM, CCF, or DIS when additional information or clarification is required regarding derogatory information in the application or the maintenance of security clearance? (Ref: AR 380-67 and AR 380-5.)	_____	_____
13. Are procedures established for reporting individuals who have access to sensitive compartmented information or other sensitive programs and are being involuntarily separated from the military or Federal service? (Ref: AR 380-67.)	_____	_____
14. Are procedures in effect to ensure that personnel are not processed for security reinvestigations that are within 12 months of retirement? (Ref: AR 380-67.)	_____	_____
15. Are initial briefings administered to personnel who require access to classified information? (Ref: AR 380-67.)	_____	_____
16. Are refresher briefings administered to personnel who require access to classified information on an annual basis? (Ref: AR 380-67.)	_____	_____
17. Are foreign travel briefings administered to personnel who hold security clearances? (Ref: AR 380-67.)	_____	_____

	GO Yes	NO GO No
18. Are records of foreign travel maintained for a 5-year period? (Ref: AR 380-67.)	_____	_____
19. Are security termination briefings administered to personnel upon termination of employment or withdrawal of security clearance, revocation of security clearance, or when absent from employment for more than 60 days? (Ref: AR 380-67.)	_____	_____
20. Is DA Form 2962 (Security Termination Statement) utilized for termination briefings? (Ref: AR 380-67.)	_____	_____
21. Is DA Form 2962 maintained by the activity for a period of 2 years after given a termination briefing? (Ref: AR 380-67.)	_____	_____
22. Are personnel security investigative records destroyed as required? (Ref: AR 380-67.)	_____	_____

Remarks

Unit Point of Contact (Name, Grade, and Organization)

Inspector (Name, Grade, and Organization)

Appendix A
References

Section I
Required Publications

AR 5-9
Area Support Responsibilities. (Cited in paras 16-2a and 19-2a.)

AR 25-55
The Department of the Army Freedom of Information Act Program. (Cited in para 10-1b.)

AR 25-400-2
The Modern Army Recordkeeping System (MARKS). (Cited in para 3-7b.)

AR 190-11
Physical Security of Arms, Ammunition, and Explosives. (Cited in paras 16-4c(1), 17-1, 17-3a, 17-4b, 17-8a(2), 20-1i, and 20-3.)

AR 190-13
The Army Physical Security Program. (Cited in paras 16-1a, 19-2a, and 20-2.)

AR 190-51
Security of Unclassified Army Property (Sensitive and Nonsensitive). (Cited in paras 16-1a, 16-4c(1), 16-7, 16-12b(1), 16-12b(2), 16-14a(1), 16-16a(3), 16-17b, 20-2, and 20-3.)

AR 380-5
Department of the Army Information Security Program. (Cited in paras 1-5k, 2-1c, 2-2a(8), 2-2b(4), 4-1, 4-2, 4-2a, 4-2b, 4-3b, 4-3c, 4-6, 4-7d, 4-8a, 4-10d(5)(d), 4-12c(2), 5-1a, 5-1b, 5-2a, 5-2e, 5-2f, 5-2g, 5-3, 5-4k, 5-5a(1), 5-5a(2), 5-5a(3), 5-5a(4), 5-5a(5), 5-5a(6), 5-5a(7), 5-5a(8), 5-5a(9), 5-5a(10), 5-5c(1), 5-5c(2), 5-5c(3), 6-1b, 6-1b(1), 6-1b(2), 6-3, 6-5b, 6-6, 8-1b, 8-2b, 9-1, 9-1a, 9-1b, 9-2a, 9-3, 9-4, 9-5, 12-1b, 16-1a, 16-7h, 16-17a(3), 20-2, 20-5, and 20-6.)

AR 380-10
Foreign Disclosure, Technology Transfer, and Contacts With Foreign Representatives. (Cited in paras 4-10g, 4-10h, and 4-11d(8).)

AR 380-15
(C) Safeguarding Classified NATO Information (U). (Cited in paras 4-12c(2) and 6-2.)

AR 380-19
Information Systems Security. (Cited in paras 5-4l(2), 12-1a, 12-1c, 12-2a, 12-2b(1), 13-1, and 14-1.)

~~**AR 380-19-1**~~
~~(C) Control of Compromising Emanations (U). (Cited in paras 12-1a and 14-1.)~~

AR 380-40
(O) Policy for Safeguarding and Controlling Communications Security (COMSEC) Material (U). (Cited in para 4-12c(2).)

AR 380-67
The Department of the Army Personnel Security Program. (Cited in paras 11-1b, 11-2b, 11-4a, 11-4b, 11-4c, 11-4e, 11-4f, 11-4g, 11-4h, 11-4i, 20-5, and 20-7.)

AR 381-10
US Army Intelligence Activities. (Cited in paras 2-7a, 2-7b, 3-7a, and 20-4.)

AR 381-12
Subversion and Espionage Directed Against the US Army (SAEDA). (Cited in paras 2-2a(5), 2-4a, 2-4c, and 20-4.)

AR 381-47
(S) US Army Offensive Counterespionage Activities (U). (Cited in para 5-5b.)

AR 525-13
(O) Antiterrorism. (Cited in paras 2-6, 16-1a, 19-2a, 19-2c, 19-2d, 19-2e, 19-7b, 19-8c, and 19-11b.)

AR 530-1
Operations Security (OPSEC). (Cited in paras 2-2a(5) and 20-6.)

AR 710-2
Supply Policy Below the Wholesale Level. (Cited in paras 16-7e and 20-1.)

AR 735-5
Policies and Procedures for Property Accountability. (Cited in para 16-17c.)

DA Pam 25-380-2
(O) Security Procedures for Controlled Cryptographic Items. (Cited in paras 20-4 and 20-5.)

DA Pam 710-2-1
Using Unit Supply System (Manual Procedures). (Cited in para 20-1.)

DOD 5220.22-M
National Industrial Security Program Operating Manual. (Cited in para 4-10d(5)(b).)

DOD 5220.22-R
Industrial Security Regulation. (Cited in para 4-10d(5)(a).)

FM 3-19.30
Physical Security. (Cited in paras 18-2a and 20-3.)

TB 380-41
(O) Procedures for Safeguarding, Accounting, and Supply Control of COMSEC Material. (Cited in para 4-12c(2).)

USAREC Reg 380-4
Security Program. (Cited in paras 18-2a, 18-3b, 19-1b, and 19-8b.)

Section II
Related Publications

AR 15-6
Procedures for Investigating Officers and Boards of Officers.

AR 40-2
Army Medical Treatment Facilities: General Administration.

AR 50-5
Nuclear and Chemical Weapons and Materiel - Nuclear Surety.

AR 50-6
Nuclear and Chemical Weapons and Materiel, Chemical Surety.

AR 190-5
Motor Vehicle Traffic Supervision.

AR 190-14
Carrying of Firearms and Use of Force for Law Enforcement and Security Duties.

AR 190-22
Searches, Seizures, and Disposition of Property.

AR 190-40
Serious Incident Report.

AR 190-47
The Army Corrections System.

AR 190-58
Personal Security.

AR 380-49
Industrial Security Program.

AR 380-53
Information Systems Security Monitoring.

AR 380-381
Special Access Programs (SAPS).

AR 381-14
~~(S)~~ (C) Technical Counterintelligence (TCI) ~~Surveillance Countermeasures (TSCM)~~ (U).

AR 381-20
The Army Counterintelligence Program.

AR 600-37
Unfavorable Information.

AR 604-10
Military Personnel Security Program.

AR 614-200
Enlisted Assignments and Utilization Management.

AR 635-200
Enlisted Personnel.

AR 680-29
Military Personnel - Organization and Type of Transaction Codes.

AR 700-84
Issue and Sale of Personal Clothing.

DA Pam 190-12
Military Working Dog Program.

DA Pam 190-51
Risk Analysis for Army Property.

DA Pam 611-21
Military Occupational Classification and Structure.

DA Pam 710-2-2
Supply Support Activity Supply System: Manual Procedures.

DOD 2000.12-H
(O) Protection of DOD Personnel and Activities Against Acts of Terrorism and Political Turbulance.

DOD 5100.76-M
Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives.

DOD 5200.1-PH-1
Classified Information Nondisclosure Agreement (SF 312) Briefing Pamphlet.

DOD 5200.8-R
Physical Security Program.

DOD 5200.28-M
ADP Security Manual, Techniques, and Procedures for Implementing, Deactivating, Testing and Evaluating - Secure Resource-Sharing ADP Systems.

DOD 5210.42-R
Nuclear Weapon Personnel Reliability Program (PRP).

DODI 5240.4
Reporting of Counterintelligence and Criminal Violations.

DOD 5400.7-R
DOD Freedom of Information Act Program.

FM 19-10
The Military Police Law and Order Operations.

FM 19-15
Civil Disturbances.

TB 5-6350-264
Selection and Application of Joint-Services Interior Intrusion Detection System (J-SIIDS).

UCMJ
Uniform Code of Military Justice.

USAREC Reg 405-1
Facility Management.

Section III
Prescribed Forms

There are no entries in this section.

Section IV
Related Forms

DA Form 873
Certificate of Clearance and/or Security Determination.

DA Form 1602
Civilian Identification.

DA Form 2062
Hand Receipt/Annex Number.

DA Form 2962
Security Termination Statement.

DA Form 3749
Equipment Receipt.

DA Form 3964
Classified Document Accountability Record.

DA Form 4283
Facilities Engineering Work Request.

DA Form 4604-R
Security Construction Statement.

DA Form 5247-R
Request for Security Determination.

DA Form 5513-R
Key Control Register and Inventory.

DA Label 87
For Official Use Only Cover Sheet.

DD Form 173/1
Joint Message Form.

DD Form 1173
Uniformed Services Identification and Privilege Card.

DD Form 1610
Request and Authorization for TDY Travel of DOD Personnel.

DD Form 1879
DOD Request for Personnel Security Investigation.

DD Form 2056
Telephone Monitoring Notification Decal.

DD Form 2501
Courier Authorization Card.

FBI Form 2-182a
Bomb Threat.

SF 50-B
Notification of Personnel Action.

SF 86
Questionnaire for National Security Positions.

SF 86A
Continuation Sheet for Questionnaire SF 86, SF 85P, and SF 85.

SF 312
Classified Information Nondisclosure Agreement.

SF 700
Security Container Information.

SF 701
Activity Security Checklist.

SF 702
Security Container Check Sheet.

SF 703
TOP SECRET Cover Sheet.

SF 704
SECRET Cover Sheet.

SF 705
CONFIDENTIAL Cover Sheet.

SF 706
TOP SECRET Label for ADP Media.

SF 707
SECRET Label for ADP Media.

SF 708
CONFIDENTIAL Label for ADP Media.

SF 710
Unclassified Label for ADP Media.

USAREC Form 1191
Master Key Inventory.

USAREC Form 1192
Key Inventory Log (Monthly and Semiannually).

USAREC Form 1193
Key Sign-In and Sign-Out Record.

Glossary

A&A
arms and ammunitions

AA&E
arms, ammunition, and explosives

AASMI
annual, announced security manager inspection

ATO
antiterrorism officer

BEQ
bachelor enlisted quarters

BICO
bomb incident control officer

BOQ
bachelor officer quarters

CCF
US Army Central Clearance Facility

CCI
controlled cryptographic item

CID
Criminal Investigation Division

CIK
crypto ignition key

COMSEC
communications security

CQ
charge of quarters

DA
Department of the Army

DCSINT
Deputy Chief of Staff for Intelligence

DEH
Directorate of Engineering and Housing

DIS
Defense Investigative Service

DOC
Director of Contracting

DOD
Department of Defense

EOD
explosive ordnance disposal

FBI
Federal Bureau of Investigation

FIA
foreign intelligence agent

FIS
foreign intelligence services

FOUO
For Official Use Only

GOV
Government-owned vehicle

GSA
General Services Administration

HQDA
Headquarters, Department of the Army

HQ RS Bde
Headquarters, United States Army Recruiting Support Brigade

HQ USAREC
Headquarters, United States Army Recruiting Command

IDS
intrusion detection system

INSCOM
US Army Intelligence and Security Command

IRP
Individual Reliability Program

JSIIDS
Joint Service Interior Intrusion Detection System

LCT
low-cost terminal

LEC
Law Enforcement Command

MP
military police

NATO
North Atlantic Treaty Organization

NCO
noncommissioned officer

NVD
night vision devices

OCA
original classification authority

OCONUS
outside continental United States

PAO
public affairs officer

PDS
protected distribution system

PMO
provost marshal office

POV
privately-owned vehicle

PR
periodic reinvestigation

PSI
personnel security investigation

PSP
Personnel Security Program

Rctg Bde
recruiting brigade

Rctg Bn
recruiting battalion

Rctg Co
recruiting company

RS
recruiting station

RS Bde
United States Army Recruiting Support Brigade

SAEDA
Subversion and Espionage Directed Against the US Army

SDNCO
staff duty noncommissioned officer

SDO
staff duty officer

SIR
serious incident report

SM
security manager

SOP
standing operating procedure

STU
secure telephone unit

TDY
temporary duty

THREATCON
terrorist threat condition

TS
TOP SECRET

TSC
Training Support Center

UADHI
unannounced after duty hours inspection

UL
Underwritersí Laboratory

USAREC
United States Army Recruiting Command

USPS
United States Postal Service