

Army Regulation 381-12

Military Intelligence

**Subversion and
Espionage
Directed
Against the U.S.
Army (SAEDA)**

**Headquarters
Department of the Army
Washington, DC
15 January 1993**

Unclassified

SUMMARY of CHANGE

AR 381-12

Subversion and Espionage Directed Against the U.S. Army (SAEDA)

This revision--

- o Requires commanders to ensure that Subversion and Espionage Directed Against the U.S. Army (SAEDA) incidents are reported to counterintelligence (CI) (1-8a).
- o Requires training to be presented by knowledgeable, qualified personnel, to the maximum extent feasible (1-8d(3)).
- o Requires training to include information on the damage that espionage has caused to national security (2-2e).
- o Expands the scope of the SAEDA special briefing to those personnel who participate in or sponsor exchange programs, commercial ventures, or treaty verification programs with foreign countries (2-3c).
- o Requires that actual or attempted illegal diversions of U.S. technology and of actual or attempted intrusions into automated information systems be reported as SAEDA incidents (3-1).
- o Encourages personnel to report the indicators of espionage as SAEDA incidents (3-3).

Effective 15 February 1993

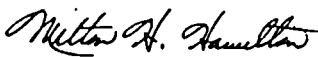
Military Intelligence

Subversion and Espionage Directed Against the U.S. Army (SAEDA)

By Order of the Secretary of the Army:

GORDON R. SULLIVAN
General, United States Army
Chief of Staff

Official:



MILTON H. HAMILTON
Administrative Assistant to the
Secretary of the Army

History. This UPDATE printing publishes a revision of this publication. Because the publication has been extensively revised, the changed portions have not been highlighted.

Summary. This regulation implements National Security Decision Directive Number 197, Reporting Hostile Contacts and Security Awareness, 1 Nov 85, and DOD Directive 5240.6, Counterintelligence Awareness and Briefing Program. It requires all Department of the Army personnel to report any incident of espionage and subversion as well as sabotage, terrorism, illegal diversion of technology, unauthorized intrusion into automated systems, and unauthorized disclosure of classified information. The regulation provides

guidance, establishes procedures, and prescribes responsibilities for the Army's counterintelligence awareness, education, and reporting program. This program is one of a number of programs designed to counter the threat of espionage and subversion against the Army.

Applicability. This regulation applies to the following elements:

- a. Active Army, Army National Guard, and U.S. Army Reserve personnel.
- b. Department of the Army civilian employees and contractors of the Department of the Army.
- c. Local national employees and Department of Defense contractors employed by Army agencies in overseas areas, as governed by Status of Forces Agreements and applicable treaties between the United States and the host countries.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff for Intelligence (DCSINT). Subject to the reservations set out below, the DCSINT has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation. The DCSINT or the Administrative Assistant to the Secretary of the Army may delegate this approval authority, in writing, to a deputy director within the proponent agency who holds the grade of colonel or the civilian equivalent. The approval authority may coordinate all questions regarding the scope of his

or her authority to approve exceptions with HQDA (DAJA-AL), WASH DC 20310-2200.

Army management control process. This regulation is not subject to the requirements of AR 11-2. It does not contain internal control provisions.

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from HQDA (DAMI-CIC), WASH DC 20310-1054.

Interim changes. Interim changes to this regulation are not official unless they are authenticated by the Administrative Assistant to the Secretary of the Army. Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQDA (DAMI-CIC), WASH DC 20310-1054.

Distribution. Distribution of this publication is made in accordance with DA Form 12-09-E, block number 3378, intended for command levels A, B, C, D, and E for the Active Army, the Army National Guard and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

Chapter 1

Introduction, page 1

Section I

Overview, page 1

Purpose • 1-1, page 1

References • 1-2, page 1

Explanation of abbreviations and terms • 1-3, page 1

Section II

Responsibilities, page 1

Deputy Chief of Staff for Intelligence, Department of the Army
• 1-4, page 1

Commanding General, U.S. Army Intelligence and Security
Command • 1-5, page 1

Commanding General, U.S. Army Training and Doctrine Command
• 1-6, page 1

Commanders of major Army Commands, Principal Officials of
Headquarters, Department of the Army, and Field Operating
Agencies • 1-7, page 1

All commanders • 1-8, page 1

Commanders of CI units • 1-9, page 1

Individual responsibilities • 1-10, page 1

Section III

Need for a SAEDA Program, page 2

The Army's vulnerability • 1-11, page 2

Importance of indicators of espionage • 1-12, page 2

Chapter 2

CI Awareness and Education, page 2

Policy • 2-1, page 2

*This regulation supersedes AR 381-12, 1 July 1981

Contents—Continued

Content of training • 2-2, *page 2*

Persons with special vulnerability • 2-3, *page 2*

Chapter 3

Reporting Requirements, *page 3*

SAEDA incidents • 3-1, *page 3*

Additional matters of CI interest • 3-2, *page 3*

Indicators of espionage • 3-3, *page 3*

Reporting procedures • 3-4, *page 4*

Statistical Reports—RCS CSGID-156 • 3-5, *page 4*

Appendixes

A. References, *page 5*

B. Countries of Special Concern, *page 5*

Glossary

Index

Chapter 1 Introduction

Section I Overview

1-1. Purpose

This regulation establishes policy, responsibilities, and procedures for the recognition and prompt reporting of incidents of attempted or actual espionage, subversion, sabotage, and terrorism directed against the U.S. Army and its personnel; of illegal diversion of technology; unauthorized intrusion into automated information systems; unauthorized disclosure of classified information; and other incidents of a counterintelligence (CI) nature. This regulation establishes the requirement for CI awareness and education. The Army's program for CI awareness, education, and reporting is known collectively as Subversion and Espionage Directed against the U.S. Army (SAEDA). The goal of the SAEDA program is to secure the assistance of every DA member in the deterrence and detection of intelligence and terrorist threats to the Army. This regulation implements DOD Directive 5240.6, Counterintelligence Awareness and Briefing Program.

1-2. References

Required and related publications and prescribed and referenced forms are listed in appendix A.

1-3. Explanation of abbreviations and terms

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

Section II Responsibilities

1-4. Deputy Chief of Staff for Intelligence, Department of the Army

The Deputy Chief of Staff for Intelligence (DCSINT), Department of the Army (DA) will—

- a. Act as DA staff proponent for the Army's CI awareness, education, and reporting program (SAEDA).
- b. Ensure Army implementation of DOD Directive 5240.6.
- c. Oversee implementation of the SAEDA program and ensure its effectiveness as a component of the Army counterintelligence program.
- d. Establish implementing policy and guidelines for the reporting, processing, and investigation of incidents reported under the SAEDA program.
- e. Ensure that the Army leadership is knowledgeable of significant SAEDA incidents and related CI matters.

1-5. Commanding General, U.S. Army Intelligence and Security Command

The Commanding General, U.S. Army Intelligence and Security Command (CG, INSCOM) will—

- a. Establish plans, programs, and procedures to implement the Army's CI awareness, education, and reporting program at echelons above corps and, when necessary and according to existing agreements, at corps and below.
- b. Conduct CI investigations and other operations resulting from SAEDA reporting worldwide according to the provisions of AR 381-47(S).
- c. Prepare and present SAEDA training tailored to the location and mission of supported units.
- d. Assist commanders in the development of continuous SAEDA publicity programs.
- e. Through U.S. Army Intelligence and Threat Analysis Center (USAITAC), disseminate to Army commanders finished intelligence on the foreign intelligence and terrorist threat which may be used as a basis for developing security countermeasures programs and to enhance CI awareness.
- f. Provide a SAEDA statistical report (RCS CSGID-156) to

HQDA (DAMI-CIC) on an annual basis as specified in paragraph 3-5.

1-6. Commanding General, U.S. Army Training and Doctrine Command

The Commanding General, U.S. Army Training and Doctrine Command (CG, TRADOC) will develop and implement standardized CI awareness programs for all initial entry courses (officer, warrant officer, and enlisted) presented by TRADOC schools and training centers.

1-7. Commanders of major Army Commands, Principal Officials of Headquarters, Department of the Army, and Field Operating Agencies

Commanders of major Army commands (MACOMs), Principal Official of Headquarters, Department of the Army, and field operating agencies (FOAs) will—

- a. Establish a SAEDA awareness and education program and ensure that all DA personnel receive SAEDA training at least annually.
- b. Ensure that all SAEDA incidents are reported according to the instructions provided herein and that emphasis is placed throughout the command on the importance of SAEDA reporting.
- c. Maintain and submit statistical data on the number of personnel who receive SAEDA training to Commander, U.S. Army Intelligence and Security Command, ATTN: IAOPS-CI, Fort Belvoir, Virginia 22060-5370, not later than 30 days following the end of each fiscal year.

1-8. All commanders

Commanders at all levels will—

- a. Ensure that known or suspected incidents of espionage and subversion, the indicators of espionage, and other reportable situations described in Chapter 3, are properly and expeditiously reported to the supporting CI office as specified herein.
- b. Ensure that knowledge of SAEDA incidents is limited by reporting incidents directly to supporting CI offices and not through command channels. This restriction is necessary in order to preserve the security of any ensuing investigation.
- c. Incorporate SAEDA training into unit training programs and ensure that all assigned and employed personnel receive annual SAEDA training. SAEDA training may be combined with other security training in order to conserve resources.
- d. Monitor the SAEDA awareness and education program to ensure that—
 - (1) The supporting Army CI office develops and presents training, to the maximum extent feasible.
 - (2) Training includes those topics required by paragraph 2-2.
 - (3) Training is prepared and/or presented by knowledgeable, qualified personnel.
 - (4) Programs for continuous publicity of the SAEDA program are developed and implemented.

1-9. Commanders of CI units

Commanders of CI units will—

- a. Establish procedures to ensure that the SAEDA program has a high priority in support to Army commanders.
- b. Identify, through liaison and other means, those personnel who should receive SAEDA special briefings as specified in paragraph 2-3 and conduct them.
- c. Ensure that SAEDA training which meets the specifications of paragraph 2-2 is prepared and presented to supported units.
- d. Obtain complete details of reported incidents and transmit or submit initial SAEDA reports as required by this regulation.

1-10. Individual responsibilities

All members of the Army, military and civilian, must be knowledgeable of their reporting responsibilities under this regulation and shall report SAEDA incidents according to chapter 3 of this regulation. This has been mandated by the President of the United States in National Security Decision Directive 197. Every individual should

know what, when, why, and where to report information required by this regulation.

Section III Need for a SAEDA Program

1-11. The Army's vulnerability

The Army is a prime and accessible target for foreign intelligence and terrorist elements which may act in a manner detrimental to the interests of our national security. The Army is vulnerable to espionage, sabotage, subversion, sedition, and terrorism from both within and outside of the United States. The dissolution of the Warsaw Pact and the retreat of Communism have not lessened the threat of espionage. The volunteer spy; the increasing need for foreign governments to collect Western technology, which they target through their intelligence services; the targeting of U.S. installations and personnel by states which sponsor terrorism; and the increasing opportunities for travel and contact between East and West, underscore the necessity for a focused and effective CI awareness, education, and reporting program.

1-12. Importance of indicators of espionage

Past espionage cases have demonstrated that co-workers and supervisors of those engaging in espionage overlooked obvious indicators of involvement in espionage which, had they been reported, would have minimized the damage to national security. Physical and information security measures designed to prevent the compromise of classified information are useless if espionage is being carried out by a trusted person within an organization. The knowledge, awareness, and participation of all DA personnel is essential to the success of the Army's SAEDA program, to the effort to counter foreign intelligence activities, and to the protection of our national security.

Chapter 2 CI Awareness and Education

2-1. Policy

All DA personnel will receive SAEDA training at least annually. Training will be conducted by qualified CI personnel, to the maximum extent feasible, as indicated below:

a. Commands not having organic CI assets will arrange for training to be conducted by supporting MACOM CI offices whenever possible. When circumstances preclude supporting CI personnel from providing training, security managers will provide the training with assistance from supporting CI offices.

b. Commands with organic CI assets will ensure that training is conducted by experienced CI personnel, if possible.

c. Sessions which include electronic media should be supplemented with training conducted by qualified CI personnel.

d. Commanders are encouraged to coordinate with supporting CI offices to develop programs to maintain a continuous level of SAEDA awareness in their units or on their installations. These programs will supplement annual training.

e. Commanders with responsibility for the security of Army special access programs and sensitive activities as specified by AR 380-381, paragraph 2-28 will develop programs to maintain a continuous level of SAEDA awareness.

2-2. Content of training

SAEDA training will be tailored specifically for the audience to which it is to be presented and to the geographic area in which it is to be given. SAEDA training may be presented at the unclassified level to ensure reaching the widest possible audience. Classified training also may be presented to cleared personnel, when appropriate. At a minimum, SAEDA training will include instructions on the following:

a. The fact that foreign intelligence services consider Army personnel to be lucrative sources of classified and sensitive unclassified

defense information. Explain how this applies to the unit or activity to which members of the audience are assigned.

b. The criminal penalties specified in the Uniform Code of Military Justice (UCMJ) and title 18 of the United States Code with regard to espionage; recent examples of persons convicted of espionage under both UCMJ and the USC and the sentences which they received; and the fact that the death penalty has been enacted under the UCMJ for espionage conducted in peacetime.

c. Methods and techniques used by foreign intelligence to place personnel under obligation and to collect information on Army facilities, activities, personnel, and technology; an explanation of the false flag approach; and examples of actual closed cases which highlight these methods.

d. The types of situations to be reported and the indicators of espionage.

e. The damage that espionage has caused to our national security, citing actual closed cases, if possible.

f. The fact that failure to report SAEDA may be used as a basis for disciplinary action under UCMJ and other authority, as applicable.

g. The 1-800 CALL SPY (1-800-225-5779) Hotline in CONUS or overseas equivalent.

h. How to respond to and report SAEDA incidents (paragraph 3-4).

i. The international and domestic terrorist threat, the vulnerability of DA personnel and their family members to terrorist acts, and the defensive measures that may be employed to thwart such acts.

j. The intelligence threat posed by nontraditional adversaries.

k. The potential intelligence threat to Department of Defense (DOD) interests posed by narcotics trafficking organizations, where applicable.

2-3. Persons with special vulnerability

a. Certain personnel present attractive targets or may be especially vulnerable to hostile approach by virtue of their position, travel, duties, access, and associations. Persons historically targeted by foreign intelligence include those who have access to sensitive compartmented, cryptographic, and special access program information. Those who occupy positions of special interest to foreign intelligence include, but are not necessarily limited to, research and development specialists; classified document custodians; and persons working in the scientific, technical, communications, and intelligence fields.

b. Special SAEDA briefings should be presented one-on-one to the individual concerned. The briefings will be conducted by CI personnel to the maximum extent feasible. The briefings should be part of the CI program where resources permit and where the potential threat is of sufficient magnitude to warrant them.

c. Security managers and supervisors will coordinate with organic or supporting CI offices to arrange the presentation of special SAEDA briefings to the following categories of personnel:

(1) DA personnel scheduled to travel to or through countries of special concern (see app B) on leave, permanent change of station, or temporary duty.

(2) DA personnel scheduled to attend international scientific, technical, engineering, or other professional meetings, especially those at which representatives of countries listed at Appendix B are likely to attend.

(3) DA personnel participating in training, education, commercial ventures, technical information sharing, or exchange programs with foreign countries, especially those listed in appendix B.

(4) DA personnel performing long-term or frequent duties in support of international treaty verification programs, those serving as military attaches in the countries listed in appendix B, and those serving abroad in U.S. embassies or diplomatic missions.

(5) Members of units or agencies which sponsor foreign scientific visitors, scientist or engineer exchange personnel, liaison officers, and students. Briefings should be presented prior to visits and to those hosting such visits.

(6) DA personnel who were born in, have resided in, or have relatives residing in the countries listed in appendix B.

d. Each special SAEDA briefing will be tailored to the particular risk involved, including inherent hazards and vulnerabilities. Special briefings will include elements of the annual briefings, as appropriate, with emphasis on reporting responsibilities.

e. CI debriefings, and one-on-one SAEDA briefings if not already conducted, will be conducted of those personnel identified in paragraphs 2–3c(1) through (5), above, as soon as feasible following completion of the travel, duty, or visit.

Chapter 3 Reporting Requirements

3–1. SAEDA incidents

Reporting of incidents and situations described in this paragraph is mandatory. Reporting procedures are specified in paragraph 3-4. Personnel subject to the UCMJ who fail to comply with the requirements of this paragraph are subject to punishment under UCMJ, as well as to adverse administrative or other adverse action authorized by applicable provisions of the United States Code or federal regulations. Personnel not subject to the UCMJ who fail to comply with the provisions of this paragraph are subject to adverse administrative action or criminal prosecution as authorized by applicable provisions of the United States Code or federal regulation. The following incidents and situations will be reported:

a. Attempts by unauthorized persons to obtain classified or unclassified information concerning U.S. Army facilities, activities, personnel, technology, or material through questioning, elicitation, trickery, bribery, threats, coercion, blackmail, photography, observation, collection of documents or material, correspondence, or computer hacking.

b. Known, suspected, or contemplated acts of espionage by Army personnel.

c. Contacts by DA personnel or their family members with persons whom they know or suspect to be members of or associated with foreign intelligence, security, or terrorist organizations. These do not include contacts which DA personnel have as a part of their official duties.

d. Contacts by DA personnel with any official or other citizen of a foreign country when that person—

(1) Exhibits excessive knowledge or undue interest about the DA member or his duties.

(2) Exhibits undue interest in U.S. technology; research, development, testing, and evaluation efforts; weapons systems; or scientific information.

(3) Attempts to obtain classified or unclassified information.

(4) Attempts to place DA personnel under obligation through special treatment, favors, gifts, money, or other means.

(5) Attempts to establish any type of business relationship that is outside the range of normal official duties.

e. All incidents in which DA personnel or their family members traveling to or through foreign countries are—

(1) Subjected to questions regarding their duties.

(2) Requested to provide military information.

(3) Threatened, coerced, or pressured in any way to cooperate with a foreign intelligence service or foreign government official.

(4) Offered assistance in gaining access to people or locations not routinely afforded Americans.

(5) Contacted by foreign government law enforcement, security, or intelligence officials.

f. Any known, suspected, or possible unauthorized disclosure or deliberate compromise of classified information, regardless of the circumstances. (The command requirements to report compromises or conduct inquiries as specified in AR 380-5, chapter VI, may also apply to these incidents).

g. Information concerning any international or domestic terrorist activity or sabotage that poses an actual or potential threat to Army or other U.S. facilities, activities, personnel, or resources.

h. Any known or suspected illegal diversion or attempted illegal diversion of U.S. technology to a foreign country.

i. Active attempts to encourage military or civilian employees to violate laws, disobey lawful orders or regulations, or disrupt military activities (subversion).

j. Known or suspected acts of treason by Army personnel.

k. Participation by Army personnel in activities advocating or teaching the overthrow of the United States by force or violence or seeking to alter the form of Government by unconstitutional means (sedition).

l. Known, suspected, or attempted intrusions into classified or unclassified automated information systems by unauthorized users or by authorized users attempting to gain unauthorized access.

m. Any situation involving coercion, influence, or pressure brought to bear on DA personnel through family members residing in foreign countries.

3–2. Additional matters of CI interest

The following are additional matters which are of CI concern and which should be reported to the nearest CI office as SAEDA incidents:

a. Discovery in a sensitive or secure area or conference room of a suspected listening device or a device which could be used for technical surveillance. DA personnel discovering such a device will not disturb it or discuss the discovery in the area where the device is located. Before taking any action, consult AR 381-14(S) for handling and reporting procedures.

b. Unauthorized or unexplained absence of DA military or civilian personnel who have had TOP SECRET, sensitive compartmented information (SCI), special access program, or TOP SECRET cryptographic access or an assignment to a special mission unit within the year preceding the absence (categorized as special category absentees for investigative and law enforcement purposes).

c. Any report of attempted or actual suicide by a DA member who has had access to classified material within one year preceding the incident.

d. COMSEC insecurities, except those which are administrative in nature (see AR 380-40, chap 7).

e. Assassination or attempted or planned assassination of anyone by terrorists or agents of a foreign power.

f. Defection, attempted defection, threats of defection, and the return to military control of U.S. military defectors.

g. Detention of DA personnel by a foreign government or entity with interests inimical to those of the United States.

h. Impersonation of Army Intelligence personnel or the unlawful possession or use of U.S. Army Intelligence identification, such as badges and credentials (investigative jurisdiction of U.S. Army Criminal Investigation Command (USACIDC) or (CID) or the Federal Bureau of Investigation (FBI)).

i. Willful compromise of the identity of U.S. Intelligence personnel engaged in clandestine intelligence and counterintelligence activities (investigative jurisdiction of CID or FBI).

j. Incidents in which foreign countries offer employment to U.S. personnel in the design, manufacture, maintenance, or employment of nuclear weapons.

3–3. Indicators of espionage

Any situation in which Army personnel exhibit any combination of the indicators of possible espionage or involvement with a foreign intelligence service as described below should be reported to CI. A single indicator by itself does not necessarily mean that a person is engaged in espionage, unless the activity associated with it is significant. If in doubt, report the situation to the supporting CI office, which will make the determination as to its significance. The following situations may be indicators of espionage:

a. Any attempt to expand access to classified information by repeatedly volunteering for assignments or duties beyond the normal scope of responsibilities or attempting to obtain information for which the person has no authorized access or need-to-know.

b. Unauthorized removal of classified materials from work area

or unauthorized possession of classified materials outside work areas, such as in residences or vehicles.

c. Extensive use of copy, facsimile, or computer equipment to reproduce or transmit classified material which may exceed job requirements.

d. Repeated or unrequired work outside of normal duty hours, especially unaccompanied.

e. Obtaining witness signatures on classified document destruction forms when the witness did not observe the destruction.

f. Bringing unauthorized cameras, recording devices, computers, or modems into areas where classified data is stored, discussed, or processed.

g. Unexplained or undue affluence, including sudden purchases of high value items (real estate, stocks, vehicles, or vacations, for example) where no logical income source exists. Attempts to explain wealth by reference to inheritance, luck in gambling, or some successful business venture.

h. Opening several bank accounts containing substantial sums of money where no logical income source exists.

i. Free spending or lavish display of wealth which appears beyond normal income.

j. Sudden reversal of financial situation or sudden repayment of large debts or loans.

k. Correspondence with persons in countries listed in appendix B.

l. Unreported contact with officials of countries listed in appendix B.

m. Frequent or unexplained trips of short duration to foreign countries.

n. Attempts to offer extra income from an outside endeavor to personnel with sensitive jobs or to entice them into criminal situations which could lead to blackmail.

o. Homesteading or repeatedly requesting extensions to tours of duty in one assignment or location, especially when the assignment offers significant access to sensitive information or the job is not desirable.

p. Repeated involvement in security violations.

q. Joking or bragging about working for a foreign intelligence service.

r. Visits to a foreign embassy, consulate, trade, or press office.

s. Business dealings with nationals or firms of countries listed in appendix B.

3-4. Reporting procedures

a. *Persons having knowledge of a SAEDA incident.*

(1) DA personnel who have been involved in or have knowledge of a SAEDA incident will report all facts immediately to the nearest supporting CI office. If these offices are not readily available, SAEDA incidents will be reported to the unit or organization security manager or commander. Security managers and commanders will ensure that, without exception, reports are relayed as securely and expeditiously as possible, but in all cases within 24 hours, to the nearest CI element.

(2) DA personnel should attempt to recall as many details regarding the incident as possible. It is recommended that pertinent details be recorded as soon as possible after the incident. Under no circumstances will they conduct their own investigation or attempt to follow the suspect. Examples of the types of information which should be reported include date, time, and place of incident; physical description of the subject; license number and description of any vehicle involved, if reasonably available; identities of any witnesses to the incident; and the details of any conversation or correspondence of a suspicious nature, if applicable. DA personnel will neither refuse nor agree to cooperate with an approach, but will remain noncommittal.

(3) Generally, SAEDA incidents will not be reported through command or Serious Incident Report channels. Exceptions are security compromises, terrorist incidents, and automated information systems intrusions, which are also reportable under AR 380-5, AR 525-13, and AR 380-19, respectively. Limiting knowledge of

SAEDA incidents is required to preserve the security of any ensuing investigation.

(4) If DA personnel are assigned or traveling outside the United States in an area where there is no Army CI element, they will report to the nearest U.S. military authority, intelligence or security officer, Defense Attache Office, or U.S. Embassy or Consulate Security Office. If the SAEDA incident is not urgent (that is, does not constitute a threat to life or property), the report will be submitted to the nearest supporting CI element upon completion of travel.

b. *CI elements.* CI elements receiving a SAEDA report will—

(1) Obtain complete details and submit an initial report to the appropriate theater sub-control office by priority or immediate electrical message or by other secure means, as urgency dictates, within 72 hours of receipt from the original source. All initial and follow-up reports will include the Army Central Control Office as an information addressee.

(2) Take no further action and make no further dissemination unless directed or approved by a control office.

(3) Inform individuals making reports that they are not to reveal the existence or nature of the incident or situation to anyone else.

(4) Submit an initial SAEDA report via secure communications, secure facsimile, or other secure means in the format specified in AR 381-47(S).

c. *Contacted personnel.* DA personnel who are contacted by another person seeking to report a SAEDA incident will follow the procedures in paragraph 3-4a, above.

d. *Information requirements control.* With the exception of statistical reports, SAEDA reports submitted under this regulation are exempt from information requirements control under AR 335-15, paragraph 5-2e(1).

3-5. Statistical Reports—RCS CSGID-156

Using data furnished by the other MACOMs and the Army Central Control Office, INSCOM will maintain a SAEDA statistical data base for use by HQDA for the purposes of monitoring and evaluating the overall effectiveness of the Army CI program. HQDA will include these statistics in status reports rendered to DOD in compliance with DOD Directive 5240.6. An annual report reflecting the following information, will be furnished to HQDA (DAMI-CIC) not later than 30 calendar days following the end of each fiscal year. (This information reporting requirement has been assigned RCS CSGID-156.)

a. Number of personnel by MACOM and agency who received SAEDA briefings during each fiscal year.

b. Number of SAEDA reports received by category.

c. Number of investigations opened as a result of SAEDA reporting.

d. Number of investigations resulting in—

(1) Planned or actual counterintelligence operations.

(2) Confirmed instances of espionage.

(3) Confirmed unauthorized disclosures of classified information or deliberate security compromises.

(4) Persons prosecuted or pending prosecution on charges of espionage or related offenses.

(5) Persons against whom administrative or judicial action was taken for failure to report incidents required by this regulation.

(6) Persons against whom administrative action was taken because of espionage-related offenses.

(7) Persons against whom administrative or judicial action was taken for other offenses resulting from reports rendered under this regulation.

e. Reports involving information on terrorist threats to the security of DOD or other U.S. interests.

f. Number of actual or attempted unauthorized intrusions into DA automated information systems.

Appendix A References

Section I Required Publications

There are no entries in this section.

Section II Related Publications

AR 380-5

Department of the Army Information Security Program

AR 380-19

Information Systems Security

AR 380-40(C)

Policy for Safeguarding and Controlling Communications Security (COMSEC) Material

AR 380-381

Special Access Programs

AR 381-10

U.S. Army Intelligence Activities

AR 381-14 (S)

Technical Surveillance Countermeasures (TSCM)

AR 381-20

U.S. Army Counterintelligence Activities.

AR 381-47 (S)

U.S. Army Counterespionage Activities (U)

AR 525-13

The Army Combatting Terrorism Program

DOD Directive 5240.6

Counterintelligence Awareness and Briefing Program

National Security Decision Directive 197

Reporting Hostile Contacts and Security Awareness

Section III

Prescribed Forms

There are no entries in this section.

Section IV

Referenced Forms

There are no entries in this section.

Iraq
Laos
Latvia
Lebanon
Libya
Lithuania
Nicaragua
North Korea
Peru
Romania
South Africa
Syria
Vietnam
States of the former USSR
Territory of the former Yugoslavia
Yanmar (formerly Burma)

Appendix B Countries of Special Concern

The following list was extracted from the Director of Central Intelligence Directive (DCID) number 1/20, Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information, dated 29 December 1991. It should be modified according to changes to the DCID.

Afghanistan
Albania
Bulgaria
People's Republic of China
Colombia
Cuba (except U.S. Naval Base)
Estonia
Iran

Glossary

Section I Abbreviations

ARNG

Army National Guard

CG

commanding general

CI

counterintelligence

CONUS

continental United States

DA

Department of the Army

DCID

Director of Central Intelligence Directive

DCSINT

Deputy Chief of Staff for Intelligence

FBI

Federal Bureau of Investigation

FIS

Foreign intelligence service

FOA

Field operating agency

HQDA

Headquarters, Department of the Army

INSCOM

U.S. Army Intelligence and Security Command

MACOM

major Army command

MI

military intelligence

SAEDA

Subversion and Espionage Directed Against the U.S. Army

SCI

Sensitive compartmented information

USACIDC

U.S. Army Criminal Investigation Command

USAITAC

U.S. Army Intelligence and Threat Analysis Center

USAR

U.S. Army Reserve

Section II Terms

Agent of a foreign power

a. Any person, other than a U.S. citizen, who—

(1) Acts in the United States as an officer

or employee of a foreign power or as a member of a group engaged in preparing for or conducting terrorist activities.

(2) Acts for or on behalf of a foreign power that engages in clandestine intelligence activities in the United States contrary to the interests of the United States, if the circumstances of the person's presence in the United States indicate that he or she may engage in such activities in the United States, or if the person knowingly aids or abets any person in conducting such activities or knowingly conspires with any person to engage in such activities.

b. Any person who—

(1) For or on behalf of a foreign power, knowingly engages in clandestine intelligence-gathering activities that involve or may involve a violation of the criminal statutes of the United States.

(2) Pursuant to the direction of an intelligence service or network of a foreign power, and for or on behalf of that power, knowingly engages in any other clandestine intelligence activities that involve or are about to involve a violation of the criminal statutes of the United States.

(3) Knowingly prepares for or engages in sabotage or international terrorism for or on behalf of a foreign power.

(4) Knowingly aids or abets any person in the conduct of the activities described above or knowingly conspires with any person to engage in the activities described above.

Clandestine intelligence activity

An activity conducted by or on behalf of a foreign power for intelligence purposes or for the purpose of affecting political or governmental processes if the activity is conducted in a manner designed to conceal from the U.S. Government the nature or fact of such activity or the role of such foreign power; also, any activity conducted in support of such activity.

Counterintelligence (CI)

Those activities which are concerned with identifying and counteracting the threat to security posed by foreign intelligence services or organizations, or by individuals engaged in espionage, sabotage, subversion or terrorism. Counterintelligence does not include, but may complement, personnel, physical, information, and communications security programs.

Counterintelligence investigation

A duly authorized, systematic, detailed examination or inquiry to uncover facts designed to determine the veracity of or to mitigate, refute, or deny information which may indicate that a person is or may have engaged in espionage or other clandestine intelligence activity, sabotage, subversion, terrorist activities, or assassinations conducted for or on behalf of a foreign power.

DA personnel

Persons employed by the Department of the Army, including military, civilian, and foreign national employees.

Deliberate compromise of classified information

The act, attempt, or reported contemplation of intentionally conveying classified documents, information, or material to any unauthorized person, including unauthorized public disclosure (18 USC 798).

Espionage

The act of obtaining, delivering, transmitting, communicating, or receiving information in respect to the national defense with an intent or reason to believe that the information may be used to the injury of the United States or to the advantage of any foreign nation (18 USC 792-798 and Article 106a, UCMJ).

False flag approach

An incident in which an officer or agent of a foreign intelligence service represents himself as a person of another nationality in order to lessen suspicion of the contact and to foster trust.

Foreign intelligence

Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons. Foreign intelligence does not include CI, except for information on international terrorist activities.

Foreign intelligence service

An organization that is part of a foreign government and engages in intelligence activities.

Foreign power

Any foreign government (regardless of whether recognized by the United States), foreign-based political party (or faction thereof), foreign military force, foreign-based terrorist group, or organization composed, in major part, of any such entity or entities.

Sabotage

An act or acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war material, premises or utilities, to include human and natural resources. (See 18 USC 2153 and DOD Directive 5240.6.)

Sedition

Participation in one or more of the following:

a. Knowingly or willfully advocating or teaching the duty or necessity of overthrowing the U.S. Government or any political subdivision therein by force or violence.

b. Printing, publishing, circulating, selling or publicly displaying written matter, with intent to cause the overthrow or destruction of any such government, which advocates or teaches the duty or necessity of such overthrow by force or violence.

c. Organizing a society or group whose

purpose is to advocate or teach the duty or necessity of such overthrow by force or violence.

d. Being or becoming a member of, or affiliated with, such society or group, knowing the purpose thereof (18 USC 2385).

Spying

In time of war, the act of clandestinely or under false pretenses collecting or attempting to collect information with the intent to convey it to a hostile party. (See Article 106, UCMJ.)

Subversion

Advocating, causing, or attempting to cause insubordination, disloyalty, mutiny, or refusal of duty by any member of the armed forces of the United States or by Department of Defense civilian personnel with the intent to interfere with, impair, or influence the loyalty, morale, or discipline of such armed forces. During time of war, subversion additionally includes:

(1) making or conveying false reports or false statements with the intent to interfere with the operation or success of the armed forces of the United States or to promote the success of its enemies; and

(2) willfully obstructing or attempting to obstruct the recruitment or enlistment service of the United States, to the injury of the United States (see 18 USC 2387-88).

Terrorist activity

Any activity that—

a. Uses violence or the threat of violence to attain goals, political, religious, or ideological in nature. This is done through intimidation, coercion, or instilling fear. Terrorism involves a criminal act that is often symbolic in nature and intended to influence an audience beyond the immediate victims.

b. Involves killing, causing serious bodily harm, kidnapping, or violently destroying property, or an attempt or credible threat to commit such an act.

c. Appears intended to endanger a protectee of the Secret Service or the Department of State or to further political, social, or economic goals by intimidating or coercing a civilian population or any segment thereof, influencing the policy of a government or international organization by intimidation or coercion, or obtaining widespread publicity for a group or its causes.

Treason

a. Violation of the allegiance owed to one's sovereign or state; betrayal of one's country.

b. Aiding or attempting to aid the enemy with arms, ammunition, supplies, money, or other things.

c. Without proper authority, knowingly harboring or protecting or giving intelligence to, communicating or corresponding with or holding any intercourse with the enemy, either directly or indirectly. See Article III,

section III, U.S. Constitution, 18 USC 2381 and Article 104, UCMJ.

Unauthorized disclosure

A communication or physical transfer of classified information to an unauthorized recipient. An unauthorized recipient is someone with no security clearance; one with a security clearance but no need to know the information; a foreign intelligence and security service; the press; criminal elements; in short, any person or organization who is not authorized access to U.S. classified information and who does not absolutely require that information to accomplish a mission in support of U. S. national security.

Section III

Special Abbreviations and Terms

There are no entries in this section.

Index

This index is organized alphabetically by topic and by subtopic within a topic. Topics and subtopics are identified by paragraph numbers.

There are no entries in this section.

Unclassified

PIN 004111-000

USAPA

ELECTRONIC PUBLISHING SYSTEM
TEXT FORMATTER ... Version 2.45

PIN: 004111-000

DATE: 11-24-98

TIME: 10:36:15

PAGES SET: 12

DATA FILE: a30.fil

DOCUMENT: AR 381-12

DOC STATUS: NEW PUBLICATION