NOV 05 2003

DEPARTMENT OF THE ARMY
MILITARY SURFACE DEPLOYMENT AND DISTRIBUTION COMMAND
OPERATIONS CENTER
661 SHEPPARD PLACE
FORT EUSTIS, VA 23604-1644

SDDC Regulation
No. 381-1

Military Intelligence
SECURITY EDUCATION PROGRAM

1. PURPOSE

This regulation prescribes policy and establishes procedures that will ensure personnel understand the security threat and are trained in appropriate countermeasures.

2. APPLICABILITY

This regulation is applicable to all Military Surface Deployment and Distribution Command (SDDC) staff elements, subordinate commands and activities including Army Reserve units OPCON to SDDC during mobilization or contingencies.

3. REFERENCES

- AR 25-2, Information Assurance
- AR 25-400-2, The Army Records Information Management System (ARIMS)
- AR 380-5, Department of the Army Information Security Program

- AR 380-67, The Department of the Army Personnel Security
- AR 381-12, Subversion and Espionage Directed Against the U.S. Army (SAEDA)
- AR 525-13, Antiterrorism
- AR 530-1, Operations Security (OPSEC)
- SDDCR 380-1, SDDC Information Security Program
- SDDCR 380-2, SDDC Operations Security (OPSEC) Program

4. TERMS

a. 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.

b. Operations Security (OPSEC). A process of analyzing friendly actions attendant to military operations and other activities to:

(1) Identify those actions that can be observed by adversary intelligence systems;

(2) Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive Critical Information (CI) in time to be useful to adversaries;

(3) Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilitites of friendly actions to adversary exploitation.

c. Subversion. A systematic attempt to overthrow or undermine a government or political system by persons working secretly within the country involved.

5. POLICY

a. The SDDC Security Education Program will be implemented at all echelons of command.

b. All command personnel, to include contractors who are assigned work space in SDDC facilities, will attend training on Antiterrorism (AT/FP Level I), Subversion and Espionage Directed Against the U.S. Army (SAEDA)(see Appendix A), Operations Security (OPSEC), and Information Security (INFOSEC) within 30 days of arrival and prior to foreign travel. Personnel will attend refresher training at least annually thereafter.

c. Antiterrorism officers will be designated at battalion and higher level units and formerly trained and certified at AT/FP Level II to conduct unit training. Battalion and brigade level commanders will receive AT/FP Level III training in the Army pre-command (PCC) training courses. Executive level personnel, who have responsibility for antiterrorism policy, planning, and execution, will be afforded opportunity to attend AT/FP Level IV seminars sponsored by the JCS. Attendance to the Level IV seminar must be coordinated through the Deputy Chief of Staff for Intelligence and Security, G2.

d. All personnel will be trained in operator's information assurance techniques prior to being granted access to Army information processing systems, and will receive refresher training at least annually.

e. Persons with access to classified defense information must receive a personnel security briefing prior to being granted access and before departing on foreign travel.

f. Security professionals will maintain a high level of proficiency through continuing education and training initiatives and participation in the Individual Development Program (IDP). See paragraph 7d for information regarding possible training courses.

6. RESPONSIBILITY

The Deputy Chief of Staff for Intelligence and Security, G2, will exercise staff supervision over the provisions of this regulation.

7. PROCEDURES

a. Staff principals and commanders/directors will ensure that:

(1) All DA personnel and contractors attend training on SAEDA, OPSEC and INFOSEC within 30 days of arrival, and at least annually thereafter. A personnel security briefing will be conducted prior to granting access to classified defense information, and before travel to a foreign country. When personnel are officially unable to attend scheduled training, the cognizant security office will be notified as to the circumstances and other arrangements will be made to provide the training.

(2) SAEDA incidents involving SDDC personnel are reported to the supporting U.S. Army Intelligence and Security Command (INSCOM) unit or supporting tactical military intelligence office. Further reporting is not required, but may be appropriate based upon the advice of the investigating Military Intelligence (MI) Special Agent.

(3) Military sponsors are encouraged to brief their family members on the contents of Army Regulations 381-12, 525-13, and 530-1. Sponsors should contact their local Security Office if assistance is desired.

b. Command/activity security officers will:

(1) Maintain liaison with intelligence support, and coordinate with the Deputy Chief of Staff for Intelligence and Security, G2, to ensure that security program educational initiatives are current, pertinent, and informative.

(2) Provide OPSEC briefings to participating personnel prior to each operation or exercise.

(3) Conduct foreign travel briefings (see Appendix B) in accordance with SDDCR 380-1 for all personnel contemplating travel to foreign countries. The foreign travel briefing must include information on antiterrorism, personal security, and SAEDA (see Appendix C).

(4) Arrange or conduct formal SAEDA training sessions for all assigned DA personnel at least annually. When feasible, SAEDA briefings will be given by an INSCOM representative.

(5) Make every effort to combine the required training sessions in order to reduce interruptions to SDDC operations.

(6) Ensure the training material contained in the appendices of this regulation is updated and supplemented as necessary based on the nature of the threat.

(7) Maintain training records to reflect the type of training received, for example, "One hour training session, 15 May 06, conducted by Resident MI Office, Norfolk, VA" or "Thirty minute security briefing provided by Command Security Officer." Training and briefing records will be maintained in accordance with AR 25-400-2, The Army Records Information Management System (ARIMS), and are subject to review during security inspections and surveys.

c. A SAEDA statistical report in accordance with AR 381-12 (RCS CSGID156) will be submitted annually not later than 15 September to G2. Data to be reported and format for report is as follows:

(1) Total number of DA personnel within your command as of the end of the fiscal year. For the purposes of this report, DA personnel are defined as military personnel, DA civilians and Army contract personnel physically assigned work space in SDDC facilities.

(2) Total number of DA personnel briefed on SAEDA within your command during the fiscal year.

(3) Total number of SAEDA briefings conducted by personnel assigned to:

(a) INSCOM units.

(b) Tactical MI units.

(c) Local Security Officers or Security Managers.

(d) All others (specify).

(4) SAEDA briefings are defined as those briefings that contain instructions on the following:

(a) Methods and techniques used by foreign intelligence services to obtain information on Army facilities, activities, personnel or material.

(b) The fact that foreign intelligence services consider DA personnel as potential sources for U.S. defense information.

(c) The nature of the international terrorist threat, the vulnerabilities of DA personnel and their families to international terrorist acts, and the defense measures that can be used to thwart such acts.

(d) SAEDA reporting procedures.

(6) The briefing must contain information on each of the four elements specified at paragraph 7c(4) above, or it will not meet the criteria for a SAEDA briefing.

d. Security personnel will endeavor to attain subject matter expertise in security disciplines applicable to SDDC security programs. Personnel should work closely with supervisors to plan and reach individual developmental goals. SD 408-R, SDDC Individual Development Plan, should be utilized for this purpose. Typical competencies for security personnel include, but is not limited to, the following:

- Conventional Physical Security
- Antiterrorism Program Management
- Electronic Security Systems Design Course
- Seaport Security Officer Training Program
- Security Engineering Course
- Physical Security thru Environmental Design
- Information Security Management
- Classification Management
- Vulnerability Assessment Fundamentals
- DA OPSEC Officer Course
- Industrial Security Management
- American Society for Industrial Security (ASIS)
- International Association for Counterrorism & Security Professionals
- Computer Security Institute

Security personnel should also consider membership in a nationally or internationally recognized and sanctioned professional security association that publishes leading edge security technology advisories and can provide additional specialized training and networking information. Some among these are –

- American Society for Industrial Security (ASIS)
- Information Systems Security Association (ISSA)
- Security Industry Association (SIA)
- Computer Security Institute (CSI)
- National Computer Security Association (NCSA)
- International Foundation for Protection Officer (IFPO)

FOR THE COMMANDER:

TIMOTHY K. McNULTY
Colonel, TC
Chief of Staff

APPENDIX A

SUBJECT: Subversion and Espionage Directed Against the U.S. Army (SAEDA) Sample Briefing

1. It cannot be over-emphasized that a continuing positive Security Education Program is essential and is in the best interest of our national defense.

2. With this in mind, the Department of the Army published AR 381-12, titled, Subversion and Espionage Directed Against the U.S. Army (Short Titled: SAEDA). The training requirements of this regulation are intended to obtain positive results in assuring the security of national defense information.

3. You possess information which is of value to foreign governments. For this reason, intelligence agents of those governments would like to meet you. They would like to know you. They would like the opportunity to attempt to indoctrinate you and they certainly want to recruit you to furnish them with information. Don't be so naive to think that you do not have information which is of value to a foreign power. As employees and members of the Army, you possess information which could contribute directly to an assessment of the weaknesses and strengths of this country.

4. The more military information you possess, the more cautious you must be in discussing that information. There is a tendency with all people to discuss little known facts with their friends and neighbors, and sometimes even with strangers because it has an uplifting effect on their ego to be able to explain things that someone else does not know. The agents of foreign intelligence services are aware of this weakness, and I assure you that they will always appear interested and appreciative of anything you have to say.

5. The information you obtain in the office must remain in the office. If you discuss military matters with your friends and neighbors there is certainly no compulsion on their part to refrain from further discussing this information with other neighbors and friends. And so, the circle of people who are knowledgeable of this information becomes larger and larger and the foreign agent need only to talk to someone in this circle of friends to obtain the information.

6. The methods of espionage we have described so far are not new. The collection and study of publications, the recruitment of spies, the collection of statements of careless people, are avenues to information. Annually it seems, the various methods of espionage are being improved upon in terms of sophistication and effectiveness.

7. The collection of information by technical means has ranged from the electronic monitoring of radio signals and telephone lines, to the targeting of areas, with high tech listening devices, where s

ensitive defense information is discussed and/or processed. Remember, sensitive information will only be discussed in a secure environment and over secure transmission devices.

8. The principle reason for this briefing is to make certain that you know what to report, and how to report suspected or actual incidents of subversion and espionage against the U.S. Army. At a minimum, you must report the following:

a. Attempts to obtain classified or other national defense information by the observation of sensitive U.S. Army activities, by the collection of documents through contact with U.S. Military or DA Civilian personnel, or by the utilization of high technology surveillance devices.

b. Attempts by persons with known or suspected foreign intelligence services associations or backgrounds. There may be attempts to obtain national defense information through the cultivation of individual friendships or by placing individuals under some type of obligation. Situations involving money, sex, ideology and revenge are among those which could make an individual vulnerable to exploitation.

c. Attempts by individuals purporting to represent a free-world nation or agency to obtain national defense information.

9. There are two basic guidelines to follow in reporting subversion and espionage situations; avoid making any firm commitments, and report suspected incidents or situations immediately to: (enter POC and telephone number of the supporting MI office). If you cannot contact anyone, request the assistance of your Security Manager. You will then be put in contact with an MI special agent.

10. In conclusion, remember these main points:

a. You are a possible espionage target regardless of your job or the degree of worth you may feel you are to a spy. Your little bit of information just may be the piece needed to complete a complex model.

b. Do not put yourself in a compromising position that could make you vulnerable to blackmail.

c. Do not talk freely and loosely about military operations and plans. If you have special access to sensitive information, limit your discussion of it to other authorized personnel in your official duty capacity and at your specified place of duty.

d. If you suspect, but are not sure, that you have been approached by an agent of a foreign intelligence service, be on the safe side and report the circumstances as soon as you can.

APPENDIX B

SUBJECT: Foreign Travel Briefing

1. U.S. citizens, especially those with access to sensitive defense information, are important targets to foreign intelligence services. You can rest assured, there are hostile intelligence operatives constantly on the alert for opportunities to gain any kind of exploitable advantage, regardless of the country you may be visiting. It is a common practice among all foreign intelligence services to establish and maintain the names of personnel whose jobs afford them access to vital defense information in any area of special interest.

2. The majority of foreign intelligence operations are hidden behind the immunity of embassies, consulates, trade delegations, missions, and other such entities that may have contact with personnel who may be of an intelligence interest. These intelligence agencies are concentrating their efforts on obtaining information involving the scientific or advanced technologies and military capabilities of our nation.

3. Key sources of technical and scientific information are the numerous conventions, seminars, conferences, and symposiums held throughout the world, continually. Many of these functions are open for attendance by representatives from the majority of nations. These representatives are specially trained and extremely proficient in obtaining information they want without disclosing anything of significant value in return. Particular care must be exercised when presenting formal papers or participating on panels to ensure that vital defense information is not disclosed to unauthorized individuals.

4. Information is obtained by way of stringent controls over the movements of foreign personnel. Guides and interpreters may be agents of, or cooperatives with a foreign intelligence service. In fact, travelers may be "targeted" shortly after applying for a visa. Under such controlled conditions, there is little that can be done to prevent espionage efforts and harassment being directed against selected individuals. Travel agencies invariably arrange for American travelers to stay at the better class of hotels, and there is strong evidence that in many cases Americans were assigned to rooms with listening devices. Planes, cabs, even buses have been bugged, trying to get that missing piece of the puzzle. All the more reason why it is important not to discuss sensitive information outside official channels, to include the prescribed place of duty.

5. American travelers should maintain a high level of personal behavior at all times. They should remember that they are guests in a foreign country, and a representative of the United States. Care must be taken to avoid revealing sensitive information to any unauthorized person. Realizing this, shouldn't they be cautioned to moderate their drinking? Aside from creating embarrassing or even

scandalous scenes, they may, by over indulgence, set themselves up for possible compromise. There have been cases wherein inebriated persons were maneuvered into sexual activities, which were photographed and used as a basis for blackmailing them into committing espionage. This is one of the oldest and most favored methods of compromising an individual.

6. Medical or dental services should be obtained from persons or institutions recommended by U.S. Consular officials. Drugs and anesthesia have been used under the guise of medical treatment for the purpose of aiding in interrogations. After such an experience, the traveler may be completely unaware of what has happened, or may believe it was a dream.

7. While it may appear that the techniques employed by foreign intelligence services are far-fetched, illicit, or taken from "spy novels," they are in fact used in daily activities and operations. Although these techniques are sometimes revolting to an American, we must nevertheless recognize them as some of the tools which are used. This way, our awareness will enable us to be in a position to successfully counter these practices.

8. In conclusion, we must remember that some foreign intelligence services carry their espionage activities to fantastic lengths. Their efforts to develop new techniques, new concepts, and new targets are limited only by their own imagination. An individual's lack of awareness and/or discretion provides these agencies with the opportunities they seek. Be alert and take the following actions:

a. Do not:

(1) Take classified information outside SDDC faciltities unless authorized by the Command Security Manager in accordance with SDDCR 380-1.

(2) Discuss classified information, or information about classified operations, in an unofficial capacity. It is smart to keep in mind the "need-to-know" concept in every conversation with every person you encounter.

(3) Engage in black market activities, especially in the purchase of art treasures or the sale of currency.

(4) Accept letters, photographs, packages, or any material whatsoever to be taken out of the country. Request your host forward the material in the normal prescribed manner.

(5) Make any oral or written statements that might be used for propaganda purposes. Among these could be a seemingly innocuous petition, presented to you while attending a conference or other meeting.

(6) Photograph military installations, troop movements or restricted areas.

(7) Get overly friendly with tourist guides, interpreters, or other citizens, and avoid attempts by photographers to take candid pictures of you.

b. Do:

(1) While abroad, report any apparent or suspected attempts at espionage to the nearest U.S. Army Intelligence Agency, if known, or to the U.S. Embassy Security Officer of the country visited. Be frank about any situation in which you have been indiscreet or were compromised. Remember, in the United States you must report in accordance with para 7a(2) of this regulation.

(2) If possible, obtain medical or dental services from sources recommended by U.S. Consular officials. In the event emergency medical treatment is needed in an unsanctioned facility, arrange to be removed as soon as it is medically safe.

(3) Practice caution when writing letters or other correspondence. Mail may be subject to censorship and examination in hostile intelligence collection.

9. Thank you for your attention. If you have no questions, please complete the briefing certificate (see Appendix D) you have been provided.

APPENDIX C

SUBJECT: Antiterrorism Briefing

1. The intent of this briefing is to provide a synopsis of points concerning the nature of the terrorist threat, the vulnerabilities of Department of Defense personnel and their dependents to terrorism and defensive measures that can be taken to decrease the probability of becoming involved in a terrorist act. Additional information on terrorism, relative to a specific operation and/or geographic area, will be provided to personnel during operation security briefings and prior to mobilization exercises.

2. Terrorism is defined as the systematic threat or use of violence by individuals or groups against persons or property in violation of national or international law for the purpose of achieving political, social, economic, or territorial change. It is often rationalized by some philosophy, theory, or ideology, however vague, nonsensical, or unrealistic. Acts of terrorism are crimes. Targets are military and civilian, and are often symbolic in nature. The most desirable targets are both symbolic and pragmatic. The perpetrators are usually members of an organized group. Unlike other criminals though, they often claim credit for their actions. As evidenced by the World Trade Center bombing, and related threats, terrorism is very much apparent within our borders. With the availability of high technology resources such as weapons, transportation and communications, terrorist tactics are increasingly ruthless and cunning. As a result, we must raise our level of awareness and stand alert to the potential dangers that surround us.

3. Terrorist incidents mainly include assassination, bombing, kidnapping, hijacking, robbery and shooting. Robberies are usually conducted for logistical reasons, i.e., acquire intelligence, weapons, and to finance operations.

4. Terrorists would prefer to target prominent military and civilian personnel because they provide more political leverage. However, rank and position are not the only factors considered by terrorists when choosing a target individual. Generally, people like you and I are accessible, and are thought of as "soft" targets, meaning we can be vulnerable to attack and the perpetrators have a reasonably good chance of escape.

5. The following defensive measures have proven useful and effective in reducing the chances that someone could become victimized by terrorists:

a. Establish positive points of contact, and keep them informed as to your whereabouts. Get them accustomed to expecting you to arrive or call during certain periods.

b. Avoid routines by staggering or altering your daily schedule whenever possible. A different route to work, occasionally, may break the boredom of frequent travel.

c. Keep a low profile. Do nothing to invite unnecessary attention to you or your family. Your dress, conduct, and mannerisms should be inconspicuous.

d. Lock your car when unattended. When it is necessary to park your car in a commercial facility, leave only the ignition or maintenance key with the attendant. When you return for your car, take a moment to look it over for signs of anything out of place.

6. If an individual is kidnapped or becomes involved in a hostage situation, they can help themselves by doing things that will assist them in retaining some degree of control. Among those measures highly recommended are:

a. Regain your composure as soon as possible and recognize your fear. Your captors are probably as apprehensive as you are, so your actions are important. Unless there is a clear chance of success, do not attempt to flee; otherwise you may become an assassination target.

b. Take mental notes of directions, modes and times of transit, surrounding noises, and other factors such as peculiar odors to identify your location. Such information could aid in an escape or rescue operation.

c. Note the number, physical description, accents, habits, and rank structure of your captors.

d. Anticipate isolation and efforts to disorient and confuse you.

e. Try to mentally prepare yourself for the situation ahead. Stay mentally active by asking for and using common market reading and writing materials as often as possible.

f. Do not aggravate your abductors. Attempt to develop a positive relationship with them. However, avoid getting into political or ideological discussions.

g. Comply with instructions, but always maintain your dignity. In order to conserve your strength, eat what is offered to you. Establish a slow methodical routine for every task.

h. Don't be depressed if negotiation efforts appear to be taking a long time. Remember, chance of survival actually increases with time.

i. If you suspect rescue operations are underway, if possible drop to the floor and/or be still. Wait for instructions from your rescuers and follow them exactly. Don't be alarmed if initially you are treated like a hostage taker; your rescuers must sort you out from the others for their own safety.

j. Speak to no one outside of the circle of rescuers until you have been debriefed.

7. In the event a bomb threat or warning is delivered in person or received in the mail, notify your supervisor or security officer as soon as possible. If the threat or warning is received by telephone, attempt to obtain the descriptive information in Appendix E.

APPENDIX D

Date

SUBJECT: Foreign Travel Briefing Certificate

I, _____, _____, of _____, am going to travel to
NAME SSN OFFICE SYMBOL

_____, in a TDY ( ) or leave ( ) status for approximately _____ days
CITY & COUNTRY NUMBER

beginning _____. My primary mode(s) of travel will be _____.
DATE

I intend to contact the following persons at the addresses and telephone numbers indicated:

NAME	ADDRESS	TELEPHONE NUMBER

.

I have been briefed regarding hostile intelligence and terrorism threats on _____ by _____ of
DATE OFFICIAL

_____ and understand my responsibilities as set forth in the briefing.
OFFICE SYMBOL

_____
SIGNATURE OF TRAVELER

I have been debriefed regarding the above travel on _____ by _____ of _____.
DATE OFFICIAL OFFICE SYMBOL

_____
SIGNATURE OF TRAVELER

PRIVACY ACT STATEMENT

Section 6311 of Title 5 to the U.S. Code authorizes collection of this information. The primary use of this information is by management and your security office to record travel security briefings you have received. Additional disclosures of the information may be: To the Department of Labor when processing a claim for compensation regarding a job connected injury or illness; to a State unemployment compensation office regarding a claim; to Federal Life Insurance or Health Benefits carriers regarding a claim; to a Federal, State, or local law enforcement agency when your agency becomes aware of a violation or possible violation of civil or criminal law; to a Federal agency when conducting an investigation on you for employment or security reasons; to the Office of Personnel Management or General Accounting Office when the information is required for evaluation of leave administration; and to the General Services Administration in connection with its responsibilities for records management.

Where the employee identification number is your Social Security Number, collection of this information is authorized by Executive Order 9397. Furnishing the information on this form, including your Social Security Number, is voluntary, but failure to do so may result in agency disapproval of your request for a travel security briefing.

If the agency uses the information furnished on this form for purposes other than these indicated above, it may provide you with an additional statement reflecting those purposes.

PRINT NAME_____

SIGNATURE_____ DATE_____

APPENDIX E

SUBJECT: Bomb Threat Guidance and Reporting Requirements

1. Be calm and courteous. Listen carefully to the caller. Note the time and the telephone number at which the call is received. Notify supervisor or security officer by prearranged signal while caller is on the line.

2. Write exact wording of the threat:

_____.

3. Questions to ask:

__ When is bomb going to explode?

__ Where is it right now?

__ What does it look like?

__ What kind of bomb is it?

__ What will cause it to explode?

__ Did you place the bomb?

__ Why?

__ What is your address?

__ What is your name?

4. Caller's identity:

Sex: ( ) Male ( ) Female ( ) Adult ( ) Juvenile

Approximate Age___. Race_____.

Voice characteristics (may be more than one):

___Calm	___Soft	___Distinct	___Raspy	___Angry	___Loud	___Slurred
___Excited	___Laughter	___Nasal	___Ragged	___Slow	___Crying	___Clearing throat
___Rapid	___Normal	___Lisp	___Deep	___Deep breathing		___Stutter
___Accent	___Familiar	___Disguised	___Crying	___Cracking voice		___Whispered

Familiar voice? Who did it sound like? _____.

5. Origin of call:

___Local ___Booth ___Internal (from within bldg?)

___Long Distance

6. Background Sounds:

___Street noises	___Music	___Factory machinery	___Crockery	___Clear
___Animal noises	___Voices	___Motor	___House noises	___Booth
___PA System	___Static	___Office machinery	___Long Distance	

Other sounds (describe)_____.

7. Threat Language:

___Well spoken/educated ___Incoherent
___Foul ___Taped
___Irrational ___Message read by caller

8. Remarks:

_____.

9. Report call to:_____/_____.
NAME or POSITION TELEPHONE NUMBER

DATE: _/_/_.
YOUR NAME: _____.
DUTY POSITION: _____.
TELEPHONE NUMBER: _____.