SECURITY BRIEFING

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.

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. 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.

d. 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.

e. 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.

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

g. 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. All DA personnel are responsible for reporting such incidents.

h. Persons responsible for any unauthorized removals or disclosures are subject to severe sanctions. This may include action under the UCMJ or other federal statutes and, when warranted, referral for criminal prosecution.

i. 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. Don't discuss information relating to unit training, mobilization, exercise, equipment, unit readiness, etc., outside the work area.

j. 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.

k. Reproduction of classified material is prohibited unless specially approved by individuals in your organizations.

l. Classified information will **ONLY** be processed on computers officially accredited, in writing, for the processing of classified information. Contact your brigade security manager for further guidance.

m. Except as authorized by Army regulations. DA civilians and military may not engage in electronic surveillance of any kind. **DO NOT DISCUSS CLASSIFIED INFORMATION OVER AN UNSECURED TELEPHONE AND DON'T 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.

n. If you suspect or discover a technical surveillance device, take no action other than to notify the brigade security manager and USAREC Security Branch.

o. All U.S. 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.

p. Remember, you are the prime target of the foreign intelligence services. Their agents will attempt to identify and exploit any character weaknesses that you may have, i.e., financial problems. Under no circumstances should you attempt on your own pursue the development of an relationship with a person you suspect to be connected with foreign intelligence services.

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

Due to the critical nature of the USAREC mission, espionage is an ever-present threat. Historically, foreign intelligence services (FIS) are more aggressive and most effective during period 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 of foreign intelligence services. Therefore, we need to be acquainted with methods used by FIS 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 U. S. Army (SAEDA).

(1) **Subversion.** Advocating, causing, or attempting to cause insubordination, disloyalty, mutiny, or refusal of duty by any member of the Armed Forces or Defense civilian personnel with the intent to interfere with, impair, or influence the loyalty, morale, or discipline of such armed forces.

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

(3) **Directed Against the U.S. Army.** Self-explanatory.

b. Human Intelligence **(HUMINT).**

(1) Members of this country's armed forces, civilian employees, and family members are prime targets for espionage by foreign intelligence services. For that reason, it is important to remember that **WE ARE ALL POTENTIALLY SUBJECT TO APPROACH** regardless of our location, rank/grade or job.

(2) On 25 December 1991, the Soviet Union, as we have known it for the past 40 plus years ceased to exist. This event, the subsequent break-up of the WARSAW pact and attempts to implement democratic reform in former communist countries has had little, if any, impact in curtailing espionage conducted against the United States.

(3) We have also witnessed a significant increase over previous decades in the number of Americans willing to conduct espionage. Greed for money, disgruntlement, revenge, and adventure ranked high as motivating factors. Foreign Intelligence Services 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. "COOPTEES" and 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, due to large measure to the influence of detonate. Foreign countries have

sizable delegations within the U. S. who have considerable freedom of movement in which they attempt to acquire technology in all stages of development.

(5) All FIS rely heavily on the cooperation of representatives from their news services commerce – including the approximately 20,000 merchant seaman who visit U.S. ports each year, integrated personnel, tourists, educational, technical and scientific institutes, and cultural exchanges for information.

(6) When considering the threat one must consider not only the numbers of foreign intelligence agents but also, and equally important, the openness of our society. When we see information that we know to be classified in newspaper 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 $10,0000 fine, 10 years in prison, or both. Other higher penalties have been and can be imposed.

(9) By making maximum use of western technology obtained through either legitimate open sources or illicit means, countries can concentrate their assets on other activities. If they can purchase or steal technology, resources can then be diverted 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 is 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 U.S. defense spending on research, deployments, and resources.

(2) They also approach authors to solicit information or attempt to obtain invitations 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 (SIGINT).**

(1) Some Foreign countries conduct extensive signal intelligence gathering efforts, continually attempting to glean information by monitoring our telephone and radio traffic. Telephones provide an ideal pathway for information. Cellular telephones and our Defense Switch Network (DSN), 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 remaining 10 percent critical gap, foreign intelligence agents rely almost exclusively upon the human source, targeting information that 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 CONFORNTS YOU.**

(4) Another technique used is misrepresentation of status, or the "False Flag" approach where agents attempt to pass themselves off as members of a U.S. agency friendly government.

(5) We can unwittingly provide intelligence information through casual conversations which can take place in the snack bar, on a shuttle bus, McDonald's, 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 work place or in a un-cleared 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, "Which one of them has or will have the information I need?" "How can I coerce him or her to cooperate?" – "How much would it take to buy their cooperation?" If you are approached you have been carefully targeted and selected – the agent has already identified what he considers to be "your unique weakness."

(2) You won't 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 aren't that stupid and they don't 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 U.S. citizen who isn't 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/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 person's 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? Don't forget foreign travel – Is the individual constantly traveling to the same OCONUS location with no apparent reason to do so?

(4) People frequently ask why we look into a person's 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 code books 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 U.S. Army, any government employee or their dependents can become a target of a foreign intelligence approach. Our patriotism, nationalism, or pride is the attitude which aggravates and stymies the best of the world's 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 the proper need-to-know.

(6) An agent is just as interested in a PFC or a GS-5 with a copy machine as a COL or SES 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, "I 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. (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 your 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, he received an invitation to a party to be given by an embassy official. Thus began a five years friendship of sorts that ended when 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, Alexander 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 U.S. 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 U.S. 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. Gilbert's arrest was considered to be " a highly important arrest" because it illustrated "a penetration operation by a foreign intelligence service into U.S. military affairs."

(4) On 28 May 1985, John Anthony Walker and his son, Michael Lance Walker were indicted by a federal grand jury in Baltimore on 6 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 for enciphering message and also provided information on the encryption devices themselves. At least a million classified messages of the military services and U.S. 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 Oct 1987, both John and Michael pleaded guilty to espionage under a plea agreement. On 6 November 1986, John Walker was sentenced to two life terms plus ten years to served concurrently. Michael was sentenced to 25 years. John Walker's arrest was the result of an FBI tip from his former wife.

(5) On 23 August 1988, Clydee Lee Conrad, a retired army sergeant first class, was arrested in West Germany and charged 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 a 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 U.S. Army to supply classified information – one of the biggest spy rings since World War II. Conrad's recruits continued to work for him after returning to the U.S., 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 Clearance in 1978 when assigned to the U.S. 8th Infantry Division headquarters in Bad Kreuznach, Germany. Despite his administrative specialists 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 NATO's 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 Division's secret documents were kept, took suitcases stuffed with classified papers out of his 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:

EXCESS INDEBTNESS OR RECURRING FINANCIAL DIFFICULTIES

CRIMINAL OR IMMORAL CONDUCT

EXCESSIVE DRINKING OR USE OF NARCOTICS

REPETITIVE ABSENCE WITHOUT LEAVE

QUESTIONABLE OR UNAUTHORIZED CONTACT WITH REPRESENTATIVES OF FOREIGN GOVERNMENTS OR AGENCIES

MENTAL OR EMOTIONAL INSTABILITY

j. 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 U.S. Defense Attach or other Americans in the U.S. 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 Director of Plans, Training, Mobilization and Security (DPTMS), 967-0973.

(3) Do not take any further actions 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 foreign intelligence agent approaches. Ensure family members are also aware of reporting procedures.

FOREIGN TRAVEL BRIEFING

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

(1) Travel to or through countries of special concern (see Appendix B, AR 381-12, 15 Jan 93).

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

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

b. These briefing should include those incidents and situations which MUST be reported. Failure to report the following may be a basis for disciplinary action under UCMJ:

(1) Attempts by unauthorized persons to obtain classified information concerning US Army facilities, activities, personnel, or material through questioning, 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 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 countries of special concern, are approached in search of classified or unclassified information.

(5) Non-official 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, of any officials countries designated as "Countries of Special Concern"

c. Immediately report these situations/incidents immediately to the nearest INSCOM or tactical MI 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, para 3-4.

CERTIFICATE OF SECURITY / SAEDA / TERRORISM AWARENESS TRAINING

This is to certify that _____
RANK LASTNAME FIRSTNAME MI

_____ Minneapolis Recruiting Battalion has received his/her initial
SSN

Security, SAEDA and Terrorism Awareness Training. This Briefing was given in

Conjunction with:

- Inprocessing
- Deployment
- PCS
- OCONUS Leave
- Outprocessing

I realize that this briefing does not replace the Level 1 or Level 2 Anti-Terrorism

Force Protection Briefing given by the Battalion S2.

_____ _____
SIGNATURE DATE