Appendix A

COUNTER-HUMAN INTELLIGENCE TECHNIQUES AND PROCEDURES

GENERAL

Appendix A contains information on operations of CI interest, and on the C-HUMINT analysis performed by MDCI analysts. It contains basic information for the C-HUMINT agent and analyst as well as the interrogator. The appendix describes those procedures employed to conduct two types of investigations as well as the legal principles important to successful completion of investigations. The investigative techniques and legal principles are presented to help expedite investigations and keep them from being bogged down and rendered ineffective by technical and legal errors. These general principles are reinforced by investigative SOPs promulgated by those commands that conduct investigations.

CONTENTS

C-HUMINT, to include investigations, operations, collections, and analysis and production, have their own unique techniques and procedures. These techniques and procedures include—

- Basic Investigative Techniques and Procedures.
- Investigative Legal Principles.
- Technical Investigative Techniques.
- Screening, Cordon, and Search Operations.
- Personalities, Organizations, and Installations List.
- Counter-Human Intelligence Analysis.
- Personnel Security Investigations.
- Counterintelligence Investigations.

Each is covered in some detail in this appendix.

Section I

BASIC INVESTIGATIVE TECHNIQUES AND PROCEDURES

TO

Appendix A

COUNTER-HUMAN INTELLIGENCE TECHNIQUES AND PROCEDURES

A-I-1. **General.** The basic investigative techniques and procedures described in this section apply to both primary types of investigations: PSI and CI (also called SAEDA) investigations. Specific information for PSI is contained in Section VII to this appendix, while CI investigations is contained in Section VIII to this appendix.

A-I-2. **Legal Principles.**

a. Most CI investigations go beyond arrest and prosecution of suspects. If an investigation cannot evolve into a more productive CI operation, and when further exploitation is not possible, the objectives must be deterrence or prevention and prosecution of the suspects. Therefore, the procedures used during an investigation must be compatible with the requirements for prosecution.

b. Investigations must be conducted in accordance with the principles of law and the rules of evidence which govern the prosecution of any criminal activity. CI personnel must have a thorough understanding of the legal principles (see Section II to Appendix A) and procedures involved in conducting an investigation for three reasons:

(1) To strictly apply them in all investigative activity.

(2) To be guided by them in cases not foreseen, when there is no time to seek specific guidance or assistance.

(3) To be able to recognize those cases where specific guidance or assistance and approval must be obtained before proceeding further.

c. Basic legal principles will always apply to CI investigative situations. The legal principles are designed to ensure that the legal rights of subjects or suspects are observed. It is important to ensure that the potential ability to prosecute any given case is not jeopardized by illegal or improper CI investigative techniques. In addition, CI personnel involved in investigative activities must obtain advice from the Staff Judge Advocate (SJA) or legal officer to implement recent court decisions interpreting statutes and regulations.

d. In cases where prosecution is a possibility, CI investigative personnel should brief the SJA trial counsel in the initial stages of the investigation. After coordination with the SCO and obtaining command approval, it will support the prosecution's case and provide insight to the CI agent regarding case direction. AR 195-5 and FM 19-20 cover the legal aspects of gathering, handling, and controlling evidence.

A-I-3. **Investigative Techniques.** Checking files and records for pertinent information on the subject of the investigation is the first action in CI investigations. Checks should begin with local unit files and expand to include the Investigative Records Repository and other military services and civilian agencies. (No Army element will retain in its files any information which is prohibited by AR 381-10.) The full exploitation of records examination as an investigative tool depends on several factors which the CI agent must consider.

a. The CI agent must know what, where, by whom, and for what purpose records are maintained throughout the AO. Upon assignment to an operational unit, the initial orientation should stress that the agent be thoroughly familiar with records that may be of assistance in investigations.

b. Most records are available to the CI agent upon official request. If all efforts to obtain the desired information through official channels are unsuccessful, the information or records cannot be subpoenaed unless legal proceedings are initiated.

c. There are occasions when documentary information or evidence is best obtained through other investigative means. The possibility of intentional deception or false information in both official and unofficial records must always be considered. Because data is recorded in some documentary form does not in itself ensure reliability. Many recorded statistics are untrue or incorrect, particularly items of biographical data. They are often repetitious or unsubstantiated information provided by the SUBJECT himself and are not to be confused with fact.

d. Reliability of records varies considerably according to the area and the status of the agency or organization keeping the records. Records found in highly industrialized areas, for example, are more extensive and generally far more reliable than those found in underdeveloped areas. Until experience with a certain type of record has been sufficient to make a thorough evaluation, treat the information with skepticism.

e. If the record is to be used in a court or board proceeding, the manner in which it is copied, extracted, or preserved will have a bearing on its use as evidence.

f. In CI investigations, the absence of a record is often just as important as its existence. This is especially important in the investigation of biographical data furnished by the SUBJECT of a CI investigation. The systematic and meticulous examination of records to confirm or refute a SUBJECT's story is very often the best means of breaking the cover story of an enemy intelligence agent.

g. The types and content of records vary markedly with the AO. Regardless of the area, the CI agent must be aware of the types of records the agent may use in conducting investigations. Available records include police and security agencies, allied agencies, vital statistics, residence

registration, education, employment, citizenship, travel, military service, foreign military records, finance records, and organization affiliation.

(1) Police and security agencies. Some major types of records which are often of value are local, regional, and national police agencies. Most nations maintain extensive personality files covering criminals, SUBJECTs, victims, and other persons who have come to official police attention because of actual or alleged criminal activity. Police interest in precise descriptive details, including photographs and fingerprint cards, often make police records particularly valuable and usually more reliable than comparable records of other agencies. Police and security agency, files are usually divided into subcategories. The CI agent must be familiar with the records system to ensure all pertinent files actually have been checked.

(2) Allied agencies. Access to records of allied intelligence agencies often depends on the personal relationship between the CI representative and the custodian of the records of interest. Such examinations are normally the assigned responsibility of an LNO. Liaison also may be necessary with other agencies when the volume of records examinations dictate the need for a single representative of the CI element. At times it may be necessary, due to the sensitivity of a particular investigation, to conceal specific interest in a person whose name is to be checked. In this instance, the name of the individual may be submitted routinely in the midst of a lengthy list of persons (maybe five to seven) who are to be checked.

(3) Vital statistics. The recording of births, deaths, and marriages is mandatory in nearly every nation, either by national or local law. In newly developed countries, however, this information may be maintained only in family journals, bibles, or in very old records. In any case, confirmation of such dates may be important. The records sought may be filed at the local level, as is usually the case in overseas areas; or they may be kept at the state or regional level, such as with state bureaus of vital statistics in the US. Rarely will original vital statistics records on individuals be maintained centrally with a national agency.

(4) Residence registration. Some form of official residency registration is required in most nations of the world. The residence record may be for tax purposes, in which case it probably will be found on file at some local fiscal or treasury office. When the residence record is needed for police and security purposes, it is usually kept in a separate police file. Residence directories, telephone books, and utility company records also may be used.

(5) Education. Both public and private schools at all levels, from primary grades through universities, have records which can serve to verify background information. The school yearbook or comparable publication at most schools usually contains a photograph and brief resume of the activities of each graduating class member. These books are a valuable record for verification and as an aid to locating leads. Registrar records normally contain a limited amount of biographical data but a detailed account of academic activities.

(6) Employment. Personnel records usually contain information on dates of employment, positions held, salary, efficiency, reason for leaving, attendance record, special skills, and biographical and identifying data. Access to these records for CI agents is relatively simple in the US but may prove difficult in some overseas areas. In such areas, it may be possible to obtain the records through liaison with local civil authorities or through private credit and business rating

firms. Depending on the AO, there may be either local, regional, or national unemployment and social security program offices. Records of these offices often contain extensive background material. In most cases, these data represent unsubstantiated information provided by the applicant and cannot be regarded as confirmation of other data obtained from the same individual. Records of the US Social Security Administration can be obtained only by the Department of Justice through written request in cases involving high-level security investigations.

(7) Citizenship. Immigration, nationalization, passport, and similar records of all nations contain data regarding citizenship status. In most instances, an investigation has been undertaken to verify background information contained in such records; therefore, these records are generally more reliable than other types. The records of both official and private refugee welfare and assistance agencies also provide extensive details relating to the citizenship status of persons of CI interest. As a general rule, refugee records (particularly those of private welfare groups) are used as a source of leads rather than for verification of factual data, since they have been found to be unreliable in nearly all AOs.

(8) Travel. A system of access to records of international travel is especially important to CI operations in overseas areas. Such records include customs records, passport and visa applications, passenger manifests of commercial carriers, currency exchange files, transient residence registrations, private and government travel agency records, and frontier control agency files. The State Department maintains passport information on US citizens; this information is available by means of the NAC. Additionally, some units maintain records of all personal foreign travel by any assigned member.

(9) Military service. Records of current and past members of the armed services of most nations are detailed and usually accurate.

(a) CI agents will encounter no difficulty in obtaining access to US military service records on official request. If a service member changes branches, has a break in service, or is hospitalized, certain elements of information must be furnished to the control office so these records can be located for review, if necessary. For those personnel who have changed branches of service, the control office will need the individual's social security number (SSN), full name, and date and place of birth. An individual's field 201 file is retired when a break in service occurs. To obtain it for review, the control office needs the individual's full name and any former service numbers.

(b) The Adjutant General's offices or control branch files may be more complete than the individual's field 201 file, particularly if the individual has had National Guard or Reserve duty as a commissioned or warrant officer.

(c) Retired Army hospital records are filed by the hospital name and year. Consequently, the name of the hospital and the correct year are required if a search of hospital records is necessary.

(10) Foreign military records. Access to foreign military records in overseas areas may be difficult. In cases where it is not possible to examine official records, leads or pertinent information may be obtained from unofficial unit histories, commercially published documents, and

files of various veterans organizations. Since listing or claiming military service is a convenient means of accounting for periods of time spent in intelligence activities or periods of imprisonment, it is frequently a critical item in dealing with possible agents of a FIS. Special effort must be made to locate some form of record which either confirms or denies an individual's service in a particular unit or the existence of the unit at the time and place the individual claims to have served. OB and personality files of various intelligence services also may be helpful.

(11) Finance records. Finance records are an important source of information. They may provide information to indicate whether a person is living beyond one's means. They may provide numerous leads such as leave periods and places, and identification of civilian financial institutions.

(12) Organization affiliation. Many organizations maintain records which may be of value to a particular investigation. Examples are labor unions; social, scientific, and sports groups; and cultural and subversive organizations. CI agents should research these organizations. But when seeking sources of information, the CI agent must be thoroughly familiar with the organization before attempting to exploit it. Organizations are often established as front groups or cover vehicles for foreign intelligence operations.

h. Having determined which records may include information pertinent to an investigation, the CI agent must select the best means to gain access and examine or copy them.

(1) The following are the procedures a CI agent should follow to gain access to records:

(a) Contact the records custodian to inCIude medical records custodian.

(b) Use proper credentials to establish identity as a US Army Special Agent.

(c) State the purpose of the inquiry.

(d) Ask for any available information.

(2) The above procedures are commonly used in PSIs, but may also be used in certain phases of CI investigations.

(3) The CI agent may conduct local agency checks by mail or telephone when time, money, or physical constraints prevent personal contact with the local agency records custodian. This procedure is discouraged unless personal contact is impossible. However, before an arrangement of this nature begins, coordination must be made with higher headquarters and the local CI agent in charge. Liaison is reciprocal cooperation between an agency with records of interest and the unit. It may include authorization for a liaison representative to conduct records checks on an exchange basis within limitations imposed by higher headquarters. This type of liaison is normally the responsibility of a designated LNO or an additional duty for a CI agent when discreet checks are not required.

(4) There is a risk factor with records checks. Exposure of the SUBJECT's name and the fact that he is under investigation may alert the SUBJECT. One way to obtain record information

is to include the SUBJECT's name in a list of persons whose records are to be checked, thus pointing no spotlight at the SUBJECT.

A-I-4. **Interview Techniques.** The interview is a structured conversation designed to obtain information from another person who is known or believed to possess information of value to an investigation. It is an official encounter, and, as such, must be conducted in accordance with the rules of evidence and other legal principles. Persons mentioned during interviews are all potential sources of information. Therefore, the CI agent should attempt to influence this person in a positive way so he will want to provide the needed information. Establish rapport between the CI agent and the interviewee; use the proper interview techniques and the basic tools of human communication. The interview can be categorized into one of several types:

a. PSI Reference Interview.

b. PSI SUBJECT Interview.

c. CI (SAEDA) Walk-in Interview.

d. CI (SAEDA) Source Interview.

e. CI (SAEDA) SUBJECT Interview.

NOTE: PSI interviews are discussed in detail in Section VII to Appendix A; CI interviews are discussed in detail in Section VIII to Appendix A.

A-I-5. **Interrogation Techniques.** Interrogation is obtaining the maximum amount of usable information through formal and systematic questioning of an individual. Apply the principles and techniques of interrogation contained in FM 34-52 to CI interrogations. CI interrogations should be conducted by at least two CI agents.

a. The CI agent uses interrogation techniques when encountering a hostile source or SUBJECT. The self-preservation instinct is stimulated in an individual who is considered a SUBJECT. This deep-rooted reaction is frequently reflected in stubborn resistance to interrogation. The SUBJECT may consider the interrogation as a battle of wits where the SUBJECT has much to lose. The SUBJECT may look upon the CI agent as a prosecutor.

b. When interrogating a SUBJECT, the CI agent must keep in mind the two-fold objective of the interrogation:

(1) Detection and prevention of activity that threatens the security of the US Army.

(2) Collection of information of intelligence interest.

c. Generally, the CI agent works toward obtaining intelligence information from the SUBJECT, leading to a confession admissible in court.

d. When preparing for an interrogation, the CI agent should—

(1) Gather and digest (complete familiarization) all available material concerning the SUBJECT and the case.

(2) Be familiar with those legal principles and procedures which may apply to the case at hand. Legal requirements may differ depending on—

(a) Whether the US is at war or in a military occupation.

(b) SOFAs.

(c) Whether the SUBJECT is a US citizen or a member of the US Armed Forces.

(d) Whether the SUBJECT is an EPW.

(3) Determine the best way to approach the SUBJECT. Previous investigative efforts may have determined that the SUBJECT is under great psychological pressure; therefore, a friendly approach might work best. The CI agent should carefully consider the approach and the succeeding tactics, to ensure that nothing the agent does will cause the SUBJECT to confess to a crime he or she did not commit.

e. Before an interrogation, the CI agent must ensure the following:

(1) The interrogation room is available and free of distractions.

(2) If recording equipment is to be used, it is installed and operationally checked.

(3) All participants in the interrogation team are thoroughly briefed on the case and interrogation plan.

(4) Sources or other persons to be used to confront the SUBJECT are available.

(5) Arrangements are made to minimize unplanned interruptions.

(6) As appropriate, arrangements are made for the SUBJECT to be held in custody or provided billeting accommodations.

f. When conducting the interrogation, apply the basic techniques and procedures outlined in FM 34-52. The following points are important:

(1) Use background questioning to provide an opportunity to study the SUBJECT face-to-face.

(2) Avoid misinterpretation and impulsive conclusions. The fact that the person is suspected may in itself create reactions of nervousness and emotion.

(3) **Do not** allow note-taking to interfere with observing the SUBJECT's reaction.

(4) Seek out all details concerning the SUBJECT's implication in a prohibited activity.

(5) Examine each of the SUBJECT's statements for its plausibility, relationship to other statements or to known facts, and factual completeness. Discrepancies which require adjustment frequently weaken the SUBJECT's position.

(6) Attempt to uncover flaws in details not considered relevant to the issue; finding the story's weakness is the key to a successful interrogation.

(7) Build up to a planned final appeal as a sustained and convincing attack on the SUBJECT's wall of resistance. Eloquent and persuasive reasoning and presenting the facts of the case may succeed where piecemeal consideration of evidence failed to produce a confession. This appeal may be based on overwhelming evidence, on contradictions, story discrepancies, or the SUBJECT's emotional weaknesses.

(8) Obtain a sworn statement if the SUBJECT wants to confess. If the SUBJECT has been given an explanation of individual rights under Article 31, Uniform Code of Military Justice (UCMJ), or the 5th Amendment to the US Constitution, any unsworn statement normally can be used in court. If the SUBJECT is neither a US citizen nor a member of the armed forces, requirements will be stipulated in the unit's SOP.

g. CI agents may use polygraph examinations as an aid to CI interrogations and investigations of intelligence operations, but only at the direction of higher headquarters.

A-I-6. **Elicitation.** Elicitation is gaining information through direct communication, where one or more of the involved parties is not aware of the specific purpose of the conversation. Elicitation is a planned, systematic process requiring careful preparation.

a. Preparation. Always apply elicitation with a specific purpose in mind.

(1) The objective, or information desired, is the key factor in determining the SUBJECT, the elicitor, and the setting.

(2) Once the SUBJECT has been selected because of his or her access to or knowledge of the desired information, numerous areas of social and official dealings may provide the setting.

(3) Before the approach, review all available intelligence files and records, personality dossiers, and knowledge possessed by others who have previously dealt with the SUBJECT. This will help to determine the SUBJECT's background, motivation, emotions, and psychological nature.

b. Approach. Approach the SUBJECT in normal surroundings to avoid suspicion. There are two basic elicitation approaches: flattery and provocation. The following variations to these approaches may be used:

(1) By appealing to the ego, self-esteem, or prominence of the SUBJECT, you may be able to guide him or her into a conversation on the area of operation.

(2) By soliciting the SUBJECT's opinion and by insinuating that he or she is an authority on a particular topic.

(3) By adopting an unbelieving attitude, you may be able to cause the SUBJECT to explain in detail or to answer out of irritation. The CI agent should not provoke the subject to the point where rapport is broken.

(4) By inserting bits of factual information on a particular topic, you may be able to influence the SUBJECT to confirm and further expound on the topic. Use this approach carefully since it does not lend itself to sudden impulse. Careless or over use of this technique may give away more information than gained.

(5) By offering sincere and valid assistance, you may be able to determine the SUBJECT's specific area of interest.

c. Conversation. Once the approach has succeeded in opening the conversation, devise techniques to channel the conversation to the area of interest. Some common techniques include—

(1) An attempt to obtain more information by a vague, incomplete, or a general response.

(2) A request for additional information where the SUBJECT's response is unclear; for example, "I agree; however, what did you mean by...?"

(3) A hypothetical situation which can be associated with a thought or idea expressed by the SUBJECT. Many people who would make no comment concerning an actual situation will express an opinion on hypothetical situations.

A-I-7. **Opposite Sex Interview.** During the preliminary planning for an interview of a member of the opposite sex, the CI agent must place emphasis on avoiding a compromising situation. This is particularly true when the person to be questioned is a SUBJECT or is personally involved in a controversial matter.

a. Embarrassment is inherent in any situation where a member of the opposite sex questions a SUBJECT concerning intimate, personal matters. The CI agent must make provisions to have present a member of the same sex as SUBJECT when the subject matter or questions might prove embarrassing to the SUBJECT.

b. Before interrogating a member of the opposite sex, advise the individual about the right to request the presence of a person of the same sex. As an alternative, a CI agent of the same sex could conduct the interview.

c. In any event, the CI agent should ensure that a third person is present, or within constant hearing distance, during any interview of a member of the opposite sex. This person must possess the necessary security clearance for the subject matter to be discussed.

d. Should questions arise during the interview that could prove embarrassing, the CI agent, before asking such questions, should advise the individual being questioned that such questions will be asked.

e. The CI agent may have another person present during such interviews, even though the Source or SUBJECT does not make a request. If the individual being questioned objects to the presence of another individual and would be less cooperative in another person's presence, have that objection and its basis reduced to writing and signed by the Source or SUBJECT, and then have the other person in attendance withdraw. If the objection is merely to the visual presence of the third party and not to the third party listening to the statement, make provisions to have the other person in attendance within normal voice range of the place of questioning, but out of sight.

f. In those investigations where the member of the opposite sex has a recent history of serious mental or nervous disorders, another member of the opposite sex must be present during the interview.

Section II

INVESTIGATIVE LEGAL PRINCIPLES

TO

Appendix A

COUNTER-HUMAN INTELLIGENCE TECHNIQUES AND PROCEDURES

A-II-I. **General.** This section looks at the legal basis for CI activities. It begins with a short discussion of the EO and the implementing of DOD and Army regulations covering intelligence activities. Section II provides strict guidelines and procedures requiring a thorough knowledge of criminal law, methods of obtaining and processing evidence, an individual's rights, and regulation oversight. It lays the ground work for the investigative and reporting sections to follow.

a. AR 381-10 sets policies and procedures governing the conduct of intelligence activities by Army intelligence components. It proscribes certain types of activities. AR 381-20 implements EO 12333, proscribing certain types of activities and strictly regulating actions commonly referred to as special collection techniques. Currently, it is the governing regulation applicable to MI assets. Neither regulation is a mission statement nor does it task entities or individuals to collect information. Instead, they constitute rules of engagement for collecting information on US persons.

b. The importance of understanding these regulations and following its guidelines to accomplish the mission cannot be overstressed. It is imperative that the individuals requiring the collection of information read and understand the—

(1) Restrictions placed on collecting information concerning US persons.

(2) Definition of the terms "collection" and "US person."

(3) Retention and dissemination of that information.

(4) Use of special collection techniques.

(5) Process of identifying and reporting questionable activities or activities in violation of these regulations, US law, or the US Constitution.

c. CI agents should seek constant assistance from their local judge advocate on the interpretation and application of the procedural guidelines contained in these regulations. Rely only on a trained lawyer's interpretation when seeking to implement any of the special collection procedures.

d. Because of the nature of this work, CI agents must at least understand the basic legal principles. Decisions made by the CI agent are frequently guided by legal concepts. Only a CI agent who is familiar with governing legal principles is able to conduct these tasks efficiently, and within the parameters of the law.

A-II-2. **Criminal Law.** Although the Army agent's criminal investigatory responsibility is limited to crimes involving national security, the CI agent must understand general criminal law as well.

a. A crime almost always requires proof of a physical act, a mental state, and the concurrence of the act and the mental state. Criminal law is not designed to prosecute persons who commit acts without a "guilty" intent. For example, a reflex action by an epileptic would not subject the epileptic to criminal liability. Additionally, criminal law is not directed at punishing individuals who privately plan criminal activity when those plans are not combined with action.

b. The act required for criminal prosecution may be a willful actor an omission to act when so required by law. Espionage, the unauthorized receipt of classified information, is an **act** punishable as a crime. The failure to report missing classified documents is an example of an **omission** to act punishable as a crime. The law recognizes several different mental states. National security crimes frequently distinguish between specific and general intent. Specific intent requires that an individual act with one of two mental elements:

(1) Purposely, indicating a desire to cause a particular result.

(2) Knowingly, indicating that the individual is substantially certain that the act will cause the result.

c. General intent is indicated by an individual who commits an act with knowledge that an unjustifiable risk of harm will occur. This definition of general intent, and the example below, are specific to the crime of sabotage (Title 18, US Code, Sections 2151-2156) which contains both specific and general elements, and are not necessarily representative of the notion of general intent as a generic criminal law concept.

Alpha, a service member, places a bolt in the engine of an F-16 aircraft. If Alpha placed the bolt in the engine with the specific intent to harm the national defense by the loss of a combat aircraft, Alpha may be convicted of sabotage. However, if Alpha placed the bolt in the engine because of a dissatisfaction with the service, and not to harm specifically the national defense, he may still be convicted of sabotage. This is true because Alpha acted in a manner indicating that he knew that an unjustifiable risk of harm would result from the act of tampering with the aircraft. Since the loss of the aircraft would hamper the national defense effort, Alpha generally intended to commit sabotage in knowing of the risk to the national defense by the act, and yet, consciously disregarding the risk.

d. The inchoate or incomplete crimes are of particular importance to CI agents. These crimes are conspiracy, attempt to commit a specific crime, and solicitation to commit a crime.

(1) Article 81, United States Manual for Courts-Martial, 1984, identifies the following elements of conspiracy:

(a) That the accused entered into an agreement with one or more persons to commit an offense under the code.

(b) That while the agreement continued to exist, and while the accused remained a party to the agreement, the accused or at least one of the co-conspirators performed an act for the purpose of bringing about the object of the conspiracy. The overt act required for a conspiracy may be legal:

Alpha and Bravo conspire to commit espionage. Bravo rents a post office box in which classified information is to be placed to distribute to a foreign agent. At the time Bravo rents the box and before any classified material has been placed in the box, Alpha and Bravo may be arrested and charged with conspiracy to commit espionage.

(2) Article 80, United States Manual for Courts-Martial, 1984, lists the following elements of attempt:

(a) That the accused did a certain overt act.

(b) That the act was done with the specific intent to commit a certain offense under the code.

(c) That the act amounted to more than mere preparation.

(d) That the act apparently tended to effect the commission of the intended offense:

Alpha intends to commit espionage by receiving classified information from Bravo. Unknown to Alpha, Bravo is actually working for CI. Bravo provides Alpha with blank papers. Alpha is arrested as he picks up the papers. Alpha may be charged with and convicted of attempted espionage.

(3) Article 82, United States Manual for Courts-Martial, 1984, identifies the following elements of solicitation: That the accused solicited or advised a certain person or persons to commit any of the four offenses named in Article 82; and that the accused did so with the intent that the offense actually be committed.

(a) Sedition and mutiny are identified in Article 94, United States Manual for Courts-Martial, 1984, as two of the four offenses that may be solicited. CI agents must, therefore, investigate to determine whether a solicitation to commit an act of sedition or mutiny has occurred.

(b) Solicitation does not require that the substantive crime (sedition) actually be committed. The accused need only advise or encourage another to commit the substantive crime. The remaining two crimes under Article 82 are not of CI interest.

A-II-3. **Evidence.**

a. The United States Manual for Courts-Martial, 1984, contains the rules of evidence applicable in courts-martial. AR 15-6 governs most administrative proceedings. AR 15-6 limits the admissibility of evidence to it being relevant and material. The CI agent must only ask whether the particular piece of evidence tends to prove or disprove a fact of consequence in the adjudication. If it does, it is admissible in an administrative hearing. The only exception to this rule is if the evidence violates the severely limited exclusionary rules applicable to administrative hearings.

b. A respondent's confession or admission, obtained by unlawful coercion or inducement likely to affect its truthfulness, will not be accepted as evidence against that respondent in an administrative proceeding. The failure to advise a respondent of Article 31, UCMJ, or Fifth Amendment rights does not, by itself, render the confession or admission inadmissible in an administrative hearing. Evidence found as the result of a search, conducted or directed by a member of the armed forces acting in an official capacity who knew the search was illegal, will not be admissible in an administrative hearing.

c. Evidence unlawfully obtained through any of the ways covered in this appendix is generally inadmissible as evidence against the suspect or accused. Any other evidence subsequently obtained or derived as a result of this evidence is likewise inadmissible. Whether the use of a particular item in evidence violates an individual's rights is usually a complex and technical determination. The CI agent should obtain advice from the local SJA specified by the unit in its SOP.

A-II-4. **Rights.** The remainder of this section discusses the constitutional rights of a suspect or accused person during an investigation and the legal issues involved when obtaining evidence by means of interviews or interrogations, searches and seizures, and apprehensions. A violation of a person's legal rights will substantially, if not completely, reduce the chances of a successful criminal prosecution.

a. interviews and interrogations. Article 31, UCMJ, and the Fifth Amendment to the US Constitution prohibit government agents from compelling any person to incriminate oneself or to answer any question, the answer to which may tend to incriminate. One may remain absolutely silent and not answer any questions. To be admissible against a person, a confession or admission must be voluntary. A statement obtained through coercion (or other unlawful inducement) is termed involuntary. Physical violence, confinement, and interrogation to the point of exhaustion are examples of acts which may produce involuntary statements.

(1) Courts will use a "reasonable person" test to determine whether the investigator should have considered the individual a suspect and, therefore, given an advisement of rights under Article 31, UCMJ. If individuals appear confused as to their rights or their status, the CI agent should make every reasonable effort to remove the confusion. As the factors that affect a proper warning may be changed by court decision, the CI agent should seek appropriate advice on a continuing basis from a judge advocate. Under Article 31, UCMJ, anyone subject to the UCMJ who is suspected of a crime and who is interviewed by an agent who is also subject to the UCMJ must be advised of his rights.

(2) To enforce the constitutional prohibition against psychologically coerced confessions, Congress, the Supreme Court, and the Court of Criminal Appeals (formerly Court of Military Appeals) have acted to require government agents to advise all suspects and accused persons of their legal rights before questioning. Failure to give the advisement, even to a suspect who is a lawyer or CI agent, will result in the exclusion of the interviewee's statements at trial. Therefore, before beginning suspect interviews, the CI agent informs the individual of his official position, the fact that the individual is a suspect or accused, and the nature of the offense of which he is accused or suspected. If unsure of the precise charge, the CI agent will explain, as specifically as possible, the nature of the facts and circumstances which have resulted in the individual's being considered a suspect.

(3) If a suspect waives the Article 31, UCMJ, rights, the government must be prepared at trial to prove that the defendant understood the rights and chose to waive them voluntarily, knowingly, and intelligently. This is a greater burden than merely showing that the suspect was read the rights and did not attempt to assert or invoke them. Whether the government can sustain this burden at trial depends largely on the testimony and written record furnished by the CI agent who conducted the interview.

(4) The explanation of rights set forth below replaces all previous explanations of legal rights, including the customary reading of Article 31, UCMJ, and the Fifth Amendment to the US Constitution. A mere recitation of this advisement, however, does not assure that subsequent statements by the suspect will be admissible in court, as it must be shown that the suspect, in fact, understood the rights.

(5) The explanation of rights will not suffice if delivered in an offhand or ambiguous manner. The tone of the interrogator's voice should not suggest that the advisement is a meaningless formality. It also would be improper for the interrogator to play down the seriousness of the investigation or play up the benefits of cooperating. In short, the interrogator must not, by words, actions, or tone of voice, attempt to induce the individual to waive the right to remain silent or the right to counsel. Such action will be denounced by the courts as contrary to the purpose of the explanation of rights requirement.

(6) The same result will occur if the interrogator accidentally misstates or confuses the provisions of the advisement. In addition, all other evidence offered will become suspect, for besides excluding illegally obtained statements, the court may reject—and administrative boards are free to reject—any evidence which is not the logical product of legally obtained statements.

(7) Tricking, deceiving, or emphasizing the benefits of cooperating with the government have not been declared illegal *per se*. The methods used must merely be directed toward obtaining a voluntary and trustworthy statement and not toward corrupting an otherwise proper Article 31, UCMJ, and the Fifth Amendment rights advisement. The CI agent administers the advisement of rights, in accordance with DA Form 3881. When the suspect appears confused or in doubt, the interrogator should give any further explanations by way of a readvisement of the rights.

(8) If the interviewee indicates a desire to consult with counsel for any reason, the interrogator should make no further attempt to continue the questioning until the suspect has

conferred with counsel or has been afforded the opportunity to do so. The interrogator may not subsequently continue the questioning unless the interviewee's counsel is present (or unless the interviewee voluntarily initiates further contact with the interrogator. If suspects decide to waive any right, such as the right to have counsel present at the interrogation or the right to remain silent, the interrogator will inform them that they may reassert their rights at any time.

(9) Under no circumstances will the suspect be questioned until the interrogator is satisfied that the individual understands the rights. The interrogator will ask the suspect to sign a waiver certificate (Part 1, DA Form 3881).

(10) If a military member, subject to the code, is suspected of an offense under the UCMJ, the person is entitled to be represented by an attorney at government expense. This can be a military lawyer of the member's choice or, if the requested lawyer is not reasonably available, a detailed military lawyer from the local Trial Defense Service Office. The suspect may also retain a civilian lawyer at no expense to the government. If an appointed counsel is refused, the suspect must have a reasonable basis for that refusal, for example, obvious incompetency. However, the suspect may not arbitrarily declare the counsel unacceptable.

(11) If the suspect requests a specific civilian lawyer, the interrogator must permit the suspect to retain one, and must not continue the interrogation unless the suspect's lawyer is present when questioning resumes, or the suspect voluntarily initiates the resumption of questioning and declines the presence of counsel. The interrogator should assist the individual in obtaining acceptable counsel. The interrogator may not limit the suspect to one telephone call or otherwise interfere in the assertion of the right to counsel.

(12) Civilians generally are not entitled to have counsel provided for them by the armed services. If a civilian suspect demands an attorney, the interrogator must permit the suspect to retain counsel. If the suspect has no lawyer, the interrogator should aid in obtaining legal counsel by providing the suspect with the names and addresses of local agencies that provide legal services.

(13) Such organizations as Legal Aid and the Lawyer's Referral Service are generally listed in local telephone directories. It is to the interrogator's advantage to aid the suspect, since the interrogator may initiate further interrogation only when the suspect is properly represented and counsel is present at the subsequent interrogation. The interrogator should direct all questions about legal representation to the local SJA.

(14) The interrogator should be prepared to question the SUBJECT about each right. Whenever possible, the interrogator should make a verbatim recording of these questions and answers. If this is not possible, the interrogator should ask the SUBJECT to acknowledge both the advisement of rights and an understanding of each right in writing.

(15) It is highly desirable to obtain oral and written acknowledgments. With evidence of both oral and written acknowledgments, the interrogator is well prepared to rebut any charge that the SUBJECT did not understand the rights.

(16) The interrogator should obtain evidence in writing that the SUBJECT made a conscious and knowledgeable decision to answer questions without a lawyer (or to speak with the assistance of a lawyer). See Figure A-II-1 for questions to ask a SUBJECT to assure an understanding of rights.

- Do you understand that you have the right to have a lawyer of your choice during this interview to advise and assist you?
- Do you also understand that your right to a military counsel means a professional lawyer and not just an officer or military superior? (Military only)
- Do you understand that the Army will provide you with a military lawyer free of charge?
- Do you understand that if you decide to answer questions that you may stop whenever you choose?
- Do you understand that anything you say will be made a matter of written record and can be used against you in a court of law?

Figure A-II-1. Questions to ask a SUBJECT to assure an understanding of the rights.

(17) If, at any time and for any reason, the SUBJECT indicates in any manner a reluctance to answer any more questions or wants to see a lawyer, the interrogator must stop immediately. The interrogator should make no attempt to persuade the SUBJECT to change his or her mind. If the SUBJECT does not want to stop the interrogation entirely, but chooses to refuse to answer some questions while answering others, the interrogator is under no obligation to continue but should certainly do so in most cases.

(18) However, the interrogator must not end the interrogation in a manner calculated to intimidate, induce, or trick the SUBJECT into answering questions that the SUBJECT does not care to answer. Under no circumstances should the interrogator ask the SUBJECT why he or she decided to reassert the rights.

(19) Article 31, UCMJ, also prohibits any use of coercion, unlawful influence, or unlawful inducement in obtaining any other evidence from a SUBJECT or accused. One general rule is that SUBJECTS may not be compelled to provide incriminating evidence against themselves through the exercise of their own mental faculties, as for example by making an oral or written statement. Conversely, a SUBJECT may be compelled to provide evidence if the form of evidence will not be affected by conscious thought, and provided the means of coercion (or compelled production) fall within the limits of fundamental decency and fairness. As examples, Article 31, UCMJ, does not prohibit the taking of the following nontestimonial evidence from SUBJECTS: fingerprints, blood samples, and handwriting or voice exemplars. These rules are often quite difficult to apply unless guidance is obtained from a legal officer or judge advocate.

(20) If a SUBJECT has been interrogated without a proper rights advisement, it is possible to correct the defect and proceed after a valid advisement of rights. If the CI agent does not know whether a prior statement was properly obtained, or does know that an impropriety occurred, the agent should provide an additional, accurate advisal of rights, and advise the SUBJECT that any statements given pursuant to defective procedures will not be admissible. This technique will minimize or eliminate the taint of the earlier errors and increase the likelihood of admissibility for the subsequent statement. (Rule 304, Manual for Courts-Martial, 1984.)

b. Search and seizure. The Fourth Amendment of the US Constitution, the Manual for Courts-Martial, and AR 381-10, Procedure 7, protect individuals against unreasonable searches and seizures of their persons, houses, papers, and effects and advises that this right will not be violated. The Fourth Amendment applies in our federal, state, and military court systems.

(1) An unlawful search is one made of a person, a person's house, papers, or effects without probable cause to believe that thereon or therein are located certain objects which are subject to lawful seizure. Probable cause to search exists when there is a reasonable belief that the person, property, or evidence sought is located in the place or on the person to be searched. It means more than "mere suspicion" or "good reason to suspect" (based, for example, on a preliminary or unsubstantiated report), but may be based on hearsay or other legally obtained information. The existence of probable cause to search permits an investigator to seek and obtain a search warrant or authorization from an appropriate judicial or military authority and conduct the desired search. The existence of probable cause may also justify an immediate search without a warrant if exigent circumstances (for example, hot pursuit into a residence, or investigation centering around an operable, movable vehicle) give rise to a reasonable belief that a delay to obtain a warrant would result in removal or destruction of the evidence.

(2) Generally, evidence found as a result of an illegal search or seizure is inadmissible in a military trial and might well taint other evidence, thus precluding further judicial action if a timely motion is made to suppress. Seek advice from the local SJA on exceptions to this rule. The legality of each search necessarily depends on all of the facts in each situation. A search may be overt or covert. The following are types of legal searches:

(a) A search conducted in accordance with the authority granted by proper search warrant is lawful. The warrant must be issued from a court or magistrate having jurisdiction over the place searched. On the installation, this may be a military judge or magistrate. Military judges and magistrates may issue search authorizations based upon probable cause pursuant to Military Rule of Evidence 315(d) and AR 27-10.

(b) A search of an individual's person, the clothing worn, and of the property in immediate possession or custody is lawful when conducted as incident to the lawful apprehension of such person.

(c) A search is lawful when made under circumstances requiring immediate action to prevent the removal or disposal of property believed on reasonable grounds to be evidence of a crime.

(d) A search is legal when made with the freely given consent of the owner in possession of the property searched. However, such consent must be the result of a knowing and

willing waiver of the rights of the individual concerned and not the mere peaceful submission to apparent lawful authority. Circumstances may dictate the need to obtain written permission of the owner to avoid later denials that permission was freely given.

(e) A commanding officer having jurisdiction over property owned or controlled by the US and under the control of an armed force may lawfully authorize the search of such property. It is immaterial whether or not the property is located in the US or a foreign country. Such a search must also be based on probable cause.

(3) For most purposes, routine physical security inspections in accordance with AR 380-5, and routine investigations of military or civilian personnel when entering or leaving military areas are not considered to be searches but are treated as legitimate administrative inspections or inventories. Contraband may be seized any time.

(4) If possible, the CI agent should request, in writing, the authority to search and should state sufficient factual information to support a conclusion that an offense has occurred or will occur and evidence of the offense is located at the place sought to be searched. Permission to search should be granted by endorsement to such a request. The law of search and seizure must always be related to the actual circumstances; the advice of an SJA or legal officer should be obtained in any doubtful case. The following procedures, however, are valid for any search:

(a) The CI agent secures all available evidence that an offense has been committed and that property relating to the offense is located at a specific place.

(b) The CI agent submits this evidence to the person with authority to order a search of the place or property.

(c) If the place or property is located in a civilian community in the US, the evidence is submitted to the judge or court with authority to issue a search warrant. To obtain a search warrant from a civilian court, CI agents must establish liaison with local civilian police agencies that are authorized to request search warrants and perform the search. The supporting SJA frequently performs a military-civilian liaison function, and should be consulted when such warrants are desired.

(d) If the place or property is located in a foreign country or occupied territory and is owned, used, or occupied by persons subject to military law or to the law of war, the evidence is submitted to a commanding officer of the US Forces who has jurisdiction over personnel subject to military law or to the law of war.

(e) If the place where the property is owned or controlled by the US is under the control of an armed force wherever located, the evidence is submitted to the commanding officer having jurisdiction over the place where the property is located.

(f) The person with authority to order a search must find in the evidence probable cause to believe that the specified place or property contains specific objects subject to lawful seizure.

(g) If the person finds probable cause, that person may then lawfully authorize the search.

(h) Having been authorized, the CI agent may search the specified place or property for the specified objects.

(5) It is possible to have a legal seizure during an illegal search. (For example, the seizure of contraband is always legal, although the illegality of the search may prevent the use of such contraband as evidence.) It is possible to have an illegal seizure during a legal search. In any given judicial procedure, the first point of inquiry will be the legality of the search. If it was illegal, there will be no need to go any further; only if the search was legal will it become necessary to determine the legality of the seizure.

(6) If the search is lawful, certain objects may be seized and admitted in evidence against the suspect:

(a) Contraband, such as property which is prohibited by law. Examples are drugs and untaxed liquor.

(b) Fruits of the crime. Property which has been wrongfully taken or possessed.

(c) Tools or means by which the crime was committed.

(d) Evidence of the crime, such as clothing.

c. Apprehension. Apprehension (called “arrest” in many civilian jurisdictions) is the taking of a person into custody. A person has been taken into custody or apprehended when his or her freedom of movement is restricted in any substantial way.

(1) Authorized individuals may apprehend persons subject to the UCMJ upon reasonable belief that an offense has been committed and that the person to be apprehended committed the offense. This is sufficient probable cause for an apprehension. The authority of the CI agent to apprehend is specified in the following documents: Article 7, UCMJ; Rule 302, Manual for Courts-Martial, 1984; and AR 381-20.

(2) The basis for arrest by civilian police depends on the particular jurisdiction concerned. In general, civilian police make arrests either—

(a) By a warrant upon a showing of probable cause to a magistrate.

(b) Without a warrant, but for probable cause, when a felony or misdemeanor is committed or attempted in their presence.

(c) If a reasonable belief exists that the person committed the offense.

(3) Incident to a lawful apprehension, the SUBJECT's person, clothing that is worn, and property in the immediate possession or control may be searched. Any weapon or means of escape may be lawfully seized.

d. Legal restrictions. For legal restrictions, see AR 381-10. For additional explanation and analysis see INSCOM Pamphlet 27-1. For explanations on proper handling of evidence, see AR 195-5 and FM 19-20. Questions should be referred to the serving SJA or legal advisor.

A-II-5. **Intelligence Oversight.**

a. AR 381-10 mandates that MI personnel conform to the spirit of the regulation in the conduct of intelligence collection. AR 381-10, Procedure 14, concisely states:

> Employees shall conduct intelligence activities only pursuant to, and in accordance with, EO 12333 and this regulation. In conducting such activities, employees shall not exceed the authorities granted the employing DOD intelligence components by law; EO, including EO 12333, and the applicable DOD and Army directives.

b. Because of this requirement, intelligence personnel have the responsibility to understand the limits of the authority under which they conduct an activity, and the procedures from the regulation that apply to the given activity.

c. AR 381-10, Procedure 15, obligates each person to report any questionable intelligence activity by electrical message through command channels to HQDA (SAIG-IO). The term "questionable activity" refers to **any** conduct that constitutes or is related to an intelligence activity that may violate the law, any EO, or any DOD or Army policy including AR 381-10.

Section III

TECHNICAL INVESTIGATIVE TECHNIQUES

TO

Appendix A

COUNTER-HUMAN INTELLIGENCE TECHNIQUES AND PROCEDURES

A-III-1. **General.** The conduct of investigations is enhanced many times by emerging sophisticated procedures designed to simplify and shorten the time required to complete certain investigative tasks while ensuring that all evidence, no matter how seemingly insignificant, is thoroughly evaluated. CI units have available to them from higher supporting echelons and from within their own resources, personnel skilled in technical investigative techniques.

a. Technical investigative techniques can contribute materially to the overall investigation. Section III identifies how each technique contributes to the total CI effort. They can assist in supplying the commander with factual information on which to base decisions concerning the security of the command. Investigators can use these techniques in connection with CI and personnel security investigations for LAAs. CI investigators selectively use the following technical services:

(1) Electronic surveillance.

(2) Investigative photography.

(3) Laboratory analysis.

(4) Polygraph (authorized for use in local access investigations).

(5) TEMPEST.

(6) Computer CE capabilities.

b. In addition, specially trained CI agents conduct TSCM investigations to detect clandestine surveillance systems. TSCM personnel and intelligence polygraph examiners are also trained and experienced CI agents.

A-III-2. **Electronic Surveillance.** Electronic surveillance is the use of electronic devices to monitor conversations, activities, sound, or electronic impulses. It is an aid in conducting investigative activities. The US Constitution; EO 12333; and AR 381-10, AR 381-14 (S), and AR 381-20 regulate the use of wiretapping and electronic eavesdropping.

a. Technical surveillance methodology, including those employed by FIS, consists of—

(1) Pickup devices. A typical system involves a transducer (such as a microphone, video camera, or similar device) to pick up sound or video images and convert them to electrical impulses. Pickup devices are available in practically any size and form. They may appear to be common items, such as fountain pens, tie clasps, wristwatches, or household or office fixtures. It is important to note that the target area does not have to be physically entered to install a pickup device. The availability of a power supply is the major limitation of pickup devices. If the device can be installed so its electrical power is drawn from the available power within the target area, there will be minimal, if any, need for someone to service the device.

(2) Transmission links. Conductors carry the impulses created by the pickup device to the listening post. In lieu of conductors, the impulses can go to a transmitter which converts the electrical impulses into a modulated radio frequency (RF) signal for transmission to the listening post. The simplest transmission system is conventional wire. Existing conductors, such as used and unused telephone and electrical wire or unground electrical conduits, may also be used. The development of miniature electronic components permits the creation of very small, easily concealed RF transmitters. Such transmitters may operate from standard power sources or may be battery operated. The devices themselves may be continuously operated or remotely activated.

(3) Listening posts. A listening post consists of an area containing the necessary equipment to receive the signals from the transmission link and process them for monitoring or recording.

(a) Listening posts use a receiver to detect the signal from an RF transmission link. The receiver converts the signal to an audio-video frequency and feeds it to the monitoring equipment. Use any radio receiver compatible with the transmitter. Receivers are small enough to be carried in pockets and may be battery operated.

(b) For wire transmission links only, a tape recorder is required. You can use many commercially available recorders in technical surveillance systems. Some of these have such features as a voice actuated start-stop and variable tape speeds (extended play). They may also have automatic volume control and can be turned on or off from a remote location.

b. Monitoring telephone conversations is one of the most productive means of surreptitious collection of information. Because a telephone is used so frequently, people tend to forget that it poses a significant security threat. Almost all telephones are susceptible to “bugging” and “tapping.”

(1) A bug is a small hidden microphone or other device used to permit monitoring of a conversation. It also allows listening to conversations in the vicinity of the telephone, even when the telephone is not in use.

(2) A telephone tap is usually a direct connection to the telephone line which permits both sides of a telephone conversation to be monitored. Tapping can be done at any point along the line, for example, at connector blocks, junction boxes, or the multiwire cables leading to a

telephone exchange or dial central office. Telephone lineman's test sets and miniature telephone monitoring devices are examples of taps. Indirect tapping of a line, requiring no physical connection to the line, may also be accomplished.

(3) The most thorough check is not absolute insurance against telephone monitoring. A dial central office or telephone exchange services all telephone lines. The circuits contained within the dial central office allow for the undetected monitoring of telephone communications. Most telephone circuits servicing interstate communications depend on microwave links. Communications via microwave links are vulnerable to intercept and intelligence exploitation.

c. Current electronic technology produces technical surveillance devices that are extremely compact, highly sophisticated, and very effective. Miniaturized technical surveillance systems are available. They can be disguised, concealed, and used by a FIS in a covert or clandestine manner. The variations of their use are limited only by the ingenuity of the technician. Equipment used in technical surveillance systems varies in size, physical appearance, and capacity. Many are identical to, and interchangeable with, components of commercially available telephones, calculators, and other electronic equipment.

A-III-3. **Investigative Photography and Video Recording.**

a. Photography and video recording in CI investigations includes—

(1) Identification of individuals. CI agents perform both overt and surreptitious photography and video recording.

(2) Recording of incident scenes. Agents photograph overall views and specific shots of items at the incident scene.

(3) Recording activities of suspects. Agents use photography and video recording to provide a record of a suspect's activities observed during surveillance or cover operations.

b. A photograph or video recording may be valuable as evidence since it presents facts in pictorial form and creates realistic mental impressions. It may present evidence more accurately than a verbal description. Photographs permit consideration of evidence which, because of size, bulk, weight, or condition, cannot be brought into the courtroom.

c. To qualify as evidence, photographs and video recordings must be relevant to the case and be free of distortion. A person who is personally acquainted with the locale, object, person, or thing represented must verify the photograph or video recording. This is usually the photographer. The agent will support photographs and video recordings used as evidence by notes made at the time of the photography These notes provide a description of what the photograph includes. The notes will contain—

(1) The case number, name of the subject, and the time and date that the photographs or video recordings were taken.

(2) Technical data, such as lighting and weather conditions and type of film, lens, and camera used.

(3) Specific references to important objects in the photograph.

d. These notes may be retained on a form such as a photo data card shown in Figure A-III-I.

e. Agents can obtain specialized photographic development support from the Intelligence Materiel Activity, Fort Meade, MD.

f Physical surveillance of US persons including photography and video recording, is governed by AR 381-10, Procedure 9.

PHOTO DATA CARD

Case number:_____ **Subject:**_____ **Photographer:**_____
Location:_____ **Date:**_____
Time of day:_____ **Weather conditions:**_____
Camera:_____ **Negative size:**_____
Lens (type):_____ **Focal length:**_____
Shutter speed:_____ **f-stop:**_____
Film:_____
Camera position:_____
A. Compass reading:_____ **B. Height and altitude:**_____
C. Lateral position:_____ **D. Tilt:**_____
E. Camera-to-subject distance:_____
Artificial light used:_____ **Developer:**_____
Developing time:_____ **Temperature:**_____ **Agitation:**_____
Method of printing:_____ **Contrast:**_____
Type of enlarger lens:_____
Paper:_____
Distances between important objectives in view:_____
Description of area:_____
_____
_____
Remarks:_____
_____
_____

Figure A-III-1. Sample photo data card.

A-III-4. **Laboratory analysis.** We must anticipate the use of false documentation and secret writing by foreign intelligence agents in many CI investigations. Detection requires specially

trained personnel and laboratory facilities. The CI unit SOP should list how this support is obtained.

A-III-5. **Polygraph.**

a. The polygraph examination is a highly structured technique conducted by specially trained CI technicians and civilians certified by proper authority as polygraph examiners. Provisions of AR 195-6 cover the polygraph program generally; AR 381-20 covers intelligence polygraphs.

(1) AR 195-6 describes general applicability, responsibilities, and use of polygraph; records processing; and selection and training of DA polygraph examiners.

(2) AR 381-20 authorizes intelligence polygraphs for CI investigations, foreign intelligence and CI operations, personnel security investigations, access to SCI, exculpation in CI and personnel security investigations; and CI scope polygraph (CSP) examinations in support of certain programs or activities listed in AR 381-20.

b. The conduct of the polygraph examination is appropriate, with respect to investigations, only when—

(1) All investigative leads and techniques have been completed as thoroughly as circumstances permit.

(2) The subject of the investigation has been interviewed or thoroughly debriefed.

(3) Verification of the information by means of polygraph is deemed essential for completion or continuation of the investigation.

c. Do not conduct a polygraph examination as a substitute for securing evidence through skillful investigation and interrogation. The polygraph examination is an investigative aid and can be used to determine questions of fact, pastor present. CI agents cannot make a determination concerning an individual's intentions or motivations, since these are states of mind, not fact. However, consider the examination results along with all other pertinent information available. Polygraph results will not be the sole basis of any final adjudication.

d. Conduct polygraph examinations during CI and personnel security investigations to—

(1) Determine if a person is attempting deception concerning issues involved in an investigation.

(2) Obtain additional leads concerning the facts of an offense, the location of items, whereabouts of persons, or involvement of other, previously unknown individuals.

(3) Compare conflicting statements.

(4) Verify statements from witnesses or subjects to include CI and personnel security investigations.

(5) Provide a just and equitable resolution of a CI or personnel security investigation when the subject of such an investigation requests an exculpatory polygraph in writing.

e. Conduct intelligence polygraph examinations to—

(1) Determine the suitability, reliability, or creditability of agents, sources, or operatives of foreign intelligence or CI operations.

(2) Determine the initial and continued eligibility of individuals for access to programs and activities authorized CSP examination support.

f. The polygraph examination consists of three basic phases: pretest, intest, and posttest.

(1) During the pretest, appropriate rights advisement are given and a written consent to undergo polygraph examination is obtained from all examinees who are suspects or accused. Advise the examinee of the Privacy Act of 1974 and the voluntary nature of examination. Conduct a detailed discussion of the issues for testing and complete the final formulation of questions to be used during testing.

(2) During the intest phase, ask previously formulated and reviewed test questions and monitor and record the examinee's responses by the polygraph instrument. Relevant questions asked during any polygraph examination must deal only with factual situations and be as simple and direct as possible. Formulate these questions so that the examinee can answer only with a yes or no. Never use or ask unreviewed questions during the test.

(3) If responses indicate deception, or unclear responses are noted during the test, conduct a posttest discussion with the examinee in an attempt to elicit information from the examinee to explain such responses.

g. A polygraph examiner may render one or more of four possible opinions concerning the polygraph examination.

(1) No opinion (NO) is rendered when less than two charts are conducted concerning the relevant issues, or a medical reason halts the examination. Normally, three charts are conducted.

(2) Inconclusive (INCL) is rendered when there is insufficient information upon which to make a determination.

(3) No deception indicated (NDI) is rendered when responses are consistent with an examinee being truthful regarding the relevant areas.

(4) Deception indicated (DI) when responses are consistent with an examinee being untruthful to the relevant test questions.

h. Certain mental or physical conditions may influence a person's suitability for polygraph examination and affect responses during testing. CI agents should report any information they possess concerning a person's mental or physical condition to the polygraph examiner before scheduling the examination. Typical conditions of concern are—

(1) Mental disorders of any type.

(2) Any history of heart, respiratory, circulatory, or nervous disorders.

(3) Any current medical disorder, to include colds, allergies, or other conditions (such as pregnancy or recent surgery).

(4) Use of drugs or alcohol before the examination.

(5) Mental or physical fatigue.

(6) Pain or physical discomfort.

i. To avoid such conditions as mental or physical fatigue, do not conduct prolonged or intensive interrogation or questioning immediately before a polygraph examination. The CI agent tells the potential examinee to continue taking any prescribed medication and bring it to the examination. Based on information provided by the CI agent and the examiner's own observations, the polygraph examiner decides whether or not a person is fit to undergo examination by polygraph. When the CI agent asks a person to undergo a polygraph examination, the person is told that the examination is voluntary and that no adverse action can be taken based solely on the refusal to undergo examination by polygraph. Further, the person is informed that no information concerning a refusal to take a polygraph examination is recorded in any personnel file or record.

j. The CI agent will make no attempt to explain anything concerning the polygraph instrument or the conduct of the examination. If asked, the CI agent should inform the person that the polygraph examiner will provide a full explanation of the instrument and all procedures before actual testing and that all test questions will be fully reviewed with the potential examinee before testing.

k. Conduct polygraph examinations in a quiet, private location. The room used for the examination must contain, as a minimum, a desk or table, a chair for the examiner, and a comfortable chair with wide arms for the examinee. The room may contain minimal, simple decorations; must have at least one blank wall; and must be located in a quiet, noise-free area. Ideally, the room should be soundproof. Visual or audio monitoring devices may be used during the examination; however, the examiner must inform the examinee that such equipment is being used and whether the examination will be monitored or recorded in any manner.

l. Normally, only the examiner and the examinee are in the room during examination. When the examinee is an accused or suspect female and the examiner is a male, a female

witness must be present to monitor the examination. The monitor may be in the examination room or may observe through audio or visual equipment, if such is available.

m. On occasion, the CI agent must arrange for an interpreter to work with the examiner. The interpreter must be fluent in English and the required language, and have a security clearance appropriate to the classification of material or information to be discussed during the examination. The interpreter should be available in sufficient time before the examination to be briefed on the polygraph procedures and to establish the proper working relationship.

n. AR 195-6 describes polygraph reports, records to be maintained, and records distribution. The CI agent must provide the examiner with all files, dossiers, and reports pertaining to the investigation or operation before the examination, and must be available to answer any questions the examiner may have concerning the case.

(1) The CI agent will not prepare any agent reports concerning the results of a polygraph examination. This does not include information derived as a result of pretest or posttest admissions, nor does it include those situations where the CI agent must be called upon by the examiner to question the subject concerning those areas which must be addressed before the completion of the examination.

(2) The polygraph examiner will prepare a DA Form 2802. A copy of this may be provided to the CI agent. Such copies must be destroyed within three months following completion of the investigation or operation. The Investigative Records Repository, Central Security Facility, Fort Meade, MD, maintains the original of the DA Form 2802. Request polygraph support in accordance with INSCOM Pamphlet 381-6.

A-III-6. **Technical Surveillance Countermeasures.**

a. TSCM versus TEMPEST. TSCM is concerned with all signals leaving a sensitive or secure area, to include audio, video, and digital or computer signals. There is a definite distinction between TSCM and TEMPEST.

(1) TEMPEST is the unintentional emanation of electronic signals outside a particular piece of equipment. Electric typewriters create such signals. The words to focus on in TEMPEST are “known” and “unintentional” emanations. TEMPEST is controlled by careful engineering or shielding.

(2) TSCM is concerned with the intentional effort to gather intelligence by foreign intelligence activities by impulsing covert or clandestine devices into a US facility, or modifying existing equipment within that area. For the most part, intelligence gained through the use of technical surveillance means will be accurate, as people are unaware they are being monitored. At the same time, the implanting of such technical surveillance devices is usually a last resort.

b. Threat. The FIS, their agents, and other persons use all available means to collect sensitive information. One way they do this is by using technical surveillance devices, commonly referred to as “bugs” and “taps.” Such devices have been found in US facilities worldwide. Security weaknesses in electronic equipment used in everyday work have also been found

worldwide. The FIS easily exploits these weaknesses to collect sensitive or classified conversations as well as the information being processed. They are interested in those things said in (supposed) confidence, since they are likely to reveal future intentions. It should be stressed that the-threat is not just audio, but video camera signals, as well as data. Devices are usually placed to make their detection almost impossible without specialized equipment and trained individuals.

c. The TSCM program. The purpose of the TSCM program is to locate and neutralize technical surveillance devices that have been targeted against US Government sensitive or secure areas. The TSCM program is designed to identify and enable the correction of exploitable technical and physical security vulnerabilities. The secondary, and closely interrelated purpose, is to provide commanders and department heads with a comprehensive evaluation of their facilities' technical and physical security postures. The Director of Central Intelligence established the requirement for a comprehensive TSCM program. DODD 5240.5 and AR 381-14(S) govern the implementation of this program.

(1) The TSCM program includes four separate functions; each with a direct bearing on the program.

(a) Detection. Realizing that the threat is there, the first and foremost function of the TSCM program is to detect these devices. Many times these devices cannot be easily detected. Occasion-ally, TSCM personnel will discover such a device by accident. When they discover a device, they must neutralize it.

(b) Nullification. Nullification includes both passive and active measures used to neutralize or negate devices that are found. An example of passive nullification is soundproofing. But soundproofing that covers only part of a room is not very helpful. Excessive wires must be removed, as they could be used as a transmission path from the room. Nullification also refers to those steps taken to make the emplacement of technical surveillance systems as difficult as possible. An example of active nullification is the removal of a device from the area.

(c) Isolation. The third function of the TSCM program is isolation. This refers to limiting the number of sensitive or secure areas and ensuring the proper construction of these areas.

(d) Education. Individuals must be aware of the foreign intelligence threat and what part they play should a technical surveillance device be detected. Additionally, people need to be alert to what is going on in and around their area, particularly during construction, renovations, and installation of new equipment.

(2) The TSCM program consists of CI technical investigations and services (such as surveys, inspections, preconstruction advice and assistance) and technical security threat briefings. TSCM investigations and services are highly specialized CI investigations and are not be to confused with compliance-oriented or administrative services conducted to determine a facility's implementation of various security directives.

(a) TSCM survey. This is an all-encompassing investigation. This investigation is a complete electronic, physical, and visual examination to detect clandestine surveillance systems. A by-product of this investigation is the identification of physical and technical security weaknesses which could be exploited by the FIS.

(b) TSCM inspection. Normally, once a TSCM survey has been conducted, it will not be repeated. If TSCM personnel note several technical and physical weaknesses during the survey, they may request and schedule an inspection at a later date. In addition, they will schedule an inspection if there has been an increased threat posed to the facility or if there is some indication that a technical penetration has occurred in the area. DODD 5240.5 specifically states that no facility will qualify automatically for recurrent TSCM support.

(c) TSCM preconstruction assistance, As with other technical areas, it is much less expensive and more effective to build in good security from the initial stages of a new project. Thus, preconstruction assistance is designed to help security and construction personnel with the specific requirements needed to ensure that a building or room will be secure and built to standards. This saves money by precluding costly changes later on.

(3) Army activities request TSCM support in accordance with AR 381-14 (S).

(a) Requests for, or references to, a TSCM investigation will be classified SECRET and marked with the protective marking, NOT RELEASABLE TO FOREIGN NATIONALS. The fact that support is scheduled, in progress, or completed, is classified SECRET.

(b) No request for TSCM support will be accepted via nonsecure means. Nonsecure telephonic discussion of TSCM support is prohibited.

(c) All requests will be considered on a case-by-case basis and should be forwarded through the appropriate major Army command to Commanding General, US Army Intelligence and Security Command, ATTN: IAOPS-CI-TC, Fort Belvoir, VA 22060-5246.

(d) When requesting or receiving support, the facility being inspected must be complete and operational, unless requesting preconstruction advice and assistance. If any additional equipment goes into the secure area after the investigation, the entire area is suspect and the investigation negated.

(e) Fully justified requests of an emergency nature, or for new facilities, may be submitted at any time, but should be submitted at least 30 days before the date the support is required. Unprogrammed requests will be funded by the requestor. Each request for unprogrammed TSCM support must be accompanied by a fund cite to defray the costs of temporary duty (TDY) and per diem.

(4) The compromise of a TSCM investigation or service is a serious security violation with potentially severe impact on national security. Do not compromise the investigation or service by any action which discloses to unauthorized persons that TSCM activity will be, is being, or has been conducted within a specific area. Unnecessary discussion of a TSCM investigation or service, particularly within the subject area, is especially dangerous.

(a) If a listening device is installed in the area, such discussion can alert persons who are conducting the surveillance and permit them to remove or deactivate their devices. When deactivated, such devices are extremely difficult to locate and may require implementation of destructive search techniques.

(b) In the event a TSCM investigation or service is compromised, the TSCM team chief will terminate the investigation or service at once. Report the circumstances surrounding the compromise of the investigation or service to the head of the serviced facility, the appropriate major Army command, and the INSCOM TSCM Program Director. TSCM personnel will not reschedule an investigation or service until the cause and impact of the compromise have been evaluated by the TSCM CI agent, the appropriate agency head, and the INSCOM TSCM Program Director.

(5) When a TSCM survey or inspection is completed, the requestor is usually given reasonable assurance that the surveyed area is free of active technical surveillance devices or hazards.

(a) TSCM personnel inform the requestor about all technical and physical security vulnerabilities with recommended regulatory corrective actions.

(b) The requestor should know that it is impossible to give positive assurance that there are-no devices in the surveyed area.

(c) The security afforded by the TSCM investigation will be nullified by the admission to the secured area of unescorted persons who lack the proper security clearance. The TSCM investigation will also be negated by—

1 Failing to maintain continuous and effective surveillance and control of the serviced area.

2 Allowing repairs or alterations by persons lacking the proper security clearance or not under the supervision of qualified personnel.

3 Introducing new furnishings or equipment without a thorough inspection by qualified personnel.

(6) Report immediately the discovery of an actual or suspected technical surveillance device via a secure means, in accordance with guidance provided in AR 381-14 (S). All information concerning the discovery will be handled at a minimum of SECRET. Installation or unit security managers will request an immediate investigation by the supporting CI unit or supporting TSCM element.

Section IV

SCREENING, CORDON, AND SEARCH OPERATIONS

TO

Appendix A

COUNTER-HUMAN INTELLIGENCE TECHNIQUES AND PROCEDURES

A-IV-1. **General.** Screening, cordon, and search operations are used to gain intelligence information. Section IV provides the techniques and procedures for these operations. Screening operations identify individuals for further interrogation by CI and interrogators. CI agents may conduct screening at MP roadblocks or checkpoints. Cordon and search operations identify and apprehend persons hostile to our operations. Actual controlling of areas is done by host nation forces assisted by CI, interrogation, and other friendly forces. In some instances, the operation may be exclusively US.

a. In a conventional combat environment, CI screening operations screen refugees, EPW, and civilian internees at mobile and static checkpoints. CI agents normally conduct these operations with other elements such as MP, interrogators, combat troops, CA, and PSYOP teams. These operations require close coordination and planning. The planning may include joint or combined planning. CI exploits cordon and search operations for individuals and information of CI interest, but is not in charge. The commander of the unit performing the cordon and search is in charge.

b. In OOTW, CI agents use cordon and search operations to ferret out the insurgent infrastructure as well as individual unit elements which may use a community or area as cover for their activities or as a support base. CI agents conduct these operations, whenever possible, with host country forces and organizations.

c. Ideally, US Forces, including CI personnel, provide support while host country officials direct the entire operation. Host country personnel should, as a minimum, be part of the screening and sweep elements on any cordon and search operation. In situations where there is no viable host nation government, these operations may be conducted unilaterally or as part of a combined force.

A-IV-2. **Counterintelligence Screening.** The purpose of CI screening operations is to identify persons of CI interest or verify persons referred by interrogators who are of CI interest, and gather information of immediate CI interest.

a. Subjects of intelligence interest. Interrogators normally conduct refugee and EPW screening at the EPW compound or refugee screening point. Interrogators refer persons identified for possible CI interest to CI personnel to be screened. CI personnel conduct interrogations with

the view to intercepting hostile intelligence agents, saboteurs, and subversives trying to infiltrate friendly lines. As the battle lines in combat change, entire segments of the population may be overrun. The local population in any area may be swelled by refugees and displaced persons (persons from other lands conscripted by enemy forces for labor). The following are examples of categories of persons of CI interest (this list is not all inclusive):

(1) Persons suspected of attempting to infiltrate through refugee flow.

(2) Line crossers.

(3) Deserters from enemy units.

(4) Persons without identification (ID) papers or forged papers (inconsistent with the norm).

(5) Repatriated prisoners of war and escapees.

(6) Members of underground resistance organizations seeking to join friendly forces.

(7) Collaborators with the enemy.

(8) Target personalities, such as those on the personalities list (also known as the black, gray, or white lists).

(9) Volunteer informants.

(10) Persons who must be questioned because they are under consideration for employment with US Forces or for appointment as civil officials by CA units.

b. Planning and coordination. CI personnel plan these screening operations, as far as possible, in conjunction with the following elements:

(1) Combat commander. The commander is concerned with channelizing refugees and EPWs through the AO, particularly in the attack, to prevent any hindrance to unit movement, or any adverse effect on unit mission.

(2) Interrogators. Interrogation personnel must understand what CI is looking for and have the commander's current PIR and information requirements (IR). Close coordination with interrogators is essential for successful CI operations.

(3) Military police. MP elements are responsible for collecting EPW and civilian internees from capturing units as far forward as possible in the AO. MP units guard the convoys transporting EPW and civilian internees to EPW camps, and command and operate the EPW camps.

(4) Civil affairs. CA elements, under the G5, are responsible for the proper disposition of refugees.

(5) Psychological operations. PSYOP elements, under the G3, contribute to screening operations by informing the populace of the need for their displacement.

(6) Civil authorities in hostile areas. Civil authorities in hostile areas are included in planning only if control has been returned to them.

c. Preparation. Before any screening operation, the CI teams involved should become intimately familiar with all available information or indicators as covered in paragraph A-IV-2f, as well as the following facts:

(1) Regulations. To have any success, CI personnel must become familiar with all restrictions placed on the civilian population within the enemy-held area, including curfews, travel restrictions, rationing, draft or conscription regulations, civilian labor force mobilization orders, required political organizational membership. Knowledge of these regulations may help the CI screener to detect discrepancies and discern changes in enemy activity.

(2) Intelligence, infrastructure, organization. In order to identify agents of the enemy intelligence or infrastructure apparatus, CI personnel must be thoroughly familiar with their methods of operation, policies, objectives, offices and suboffices, schools, officials, and known agents. This includes knowing what the enemy calls itself and its organization as well as the known names for the same organization.

(3) Order of battle. The CI team needs to maintain and have ready access to current OB information. All team members must know what adversary forces they are facing and what units are in the AO. CI teams need to know adversary unit disposition, composition, strength, weaknesses, equipment, their training, history, activities, and personalities. The better CI teams know their adversaries, the better they can employ the principles of CI in support of their own unit's mission.

(4) Area of operations. CI personnel should also become familiar with the area in which they are operating; particularly geography, landmarks, distances, and travel conditions. Knowing such pertinent information as the political situation, social and economic conditions, customs, and racial problems of the area is essential.

(5) Lists and information sheets. CI teams should distribute apprehensions lists and information sheets listing indicators of CI interest to the troops, MP, or other personnel assisting with the screening operation. CI teams should make up forms and pass them out to the individuals to be screened requiring them to record personal data. This form will aid in formulating the type of questions to be asked and in determining the informational areas needed to fulfill PIR and IR. Include the following data, plus anything else judged necessary, on the form:

(a) Full name, other names, date and place of birth, current and permanent residences, and current citizenship.

(b) The same information as above concerning the father, mother, and siblings, including the occupation and whereabouts of each.

(c) If married, the names of spouse (including female maiden name), date, place of birth (DPOB), nationality, occupation, and personal data on spouse's family.

(d) The individual's education and knowledge of languages.

(e) Details of the individual's career to include schools, military service, technical and professional qualifications, political affiliations, and countries visited.

(f) Point of departure, destination, and purpose.

NOTE: The Geneva Conventions do not require this, and if the person refuses to give the information, there is nothing that can be done about it. Prepare the form in the native language of the host nation and enemy force, if different. Ensure that it is prepared in the proper dialect of the language.

d. Main battle area screening.

(1) Capturing troops search EPWs and internees captured in the main battle area (MBA) for weapons and documents, and prepare EPW and civilian internee capture tags. MP tasked with EPW operations collect EPW and civilian internees from capturing units as far forward as possible, normally establishing a division forward EPW and civilian internee collection point in or near the brigade support area (BSA). MP are responsible for subsequent evacuation of EPWs and civilian internees to the division central collection point and further rearward to internment sites.

(2) Initial screening should take place at the brigade collecting points. The initial screening will, as a minimum, consist of interrogation by intelligence interrogation personnel. Interrogation does not take precedence over rapid evacuation of EPW and civilian internees from dangerous areas. This is required by Article 19, Geneva Convention. Segregate individuals of CI interest from other EPW and civilian internees. Identify them to evacuating MP who will refer them to a CI team at division. EPW and civilian internees of CI interest remain segregated and are referred to CI teams for coordination of more detailed interrogation as they pass through the evacuation process.

(3) Return those EPW and civilian detainees determined to be of no CI value to normal evacuation channels. Expeditiously transport EPW and civilian internees considered to be of great CI value such as officers of brigade co-remand level or higher or civilian electronics specialists or others of similar background to any desired level of interrogation.

e. Conduct. Because of time and the large numbers of people to be interrogated, it is impossible to interrogate everyone. Civilians moving about the combat area have to be subjected to brief inquiries on a selective basis by MI, CA, PSYOP, and MP personnel. Such brief inquiries are designed to locate and separate suspicious persons from the masses and should be thought of as a preliminary interrogation.

(1) While some are detained for interrogation, some selected persons are detained for further CI interrogation. Upon notification of a detainee or prisoner of CI interest, a CI team will be

dispatched as soon as possible to the collection or screening point. The CI team will then coordinate with the interrogation team to determine the best method for conducting the CI interrogation or screening. If a determination is made that the EPW or detainee is of CI interest, the CI team will either control operational activity or refer the operation to the next higher echelon. If the detainee is to be referred to a higher echelon for the detailed interrogation, furnish a preliminary screening sheet and SPOT report to the evacuating unit. The evacuating unit will deliver the detainee and screening report to the next echelon CI team.

(2) The CI screening report should include the following:

(a) Identity. Screen all identifying documents in the form of ID cards, ration cards, draft cards, driver's license, auto registration, travel documents, and passport. Record rank, service number, and unit if a person is, or has been a soldier. Check all this information against the form previously filled out by the detainee if this was done.

(b) Background. The use of the form identified earlier will aid in obtaining the information required; however, certain information areas on the forms will have to be clarified, especially if data indicate a suspect category or the person's knowledgeability of intelligence information. If the form has not been filled out at this point, try to gain the information through questioning.

(c) Recent activities. Examine the activities of persons during the days before their detainment or capture. What were they doing to make a living? What connection, if any, have they had with the enemy? Why were they in the area? This line of questioning may bring out particular skills such as those associated with a radio operator, linguist, or photographer. Make physical checks for certain types of calluses, bruises, or stains to corroborate or disprove his story. Sometimes soil on shoes will not match that from the area he claims to come from.

(d) Journey or escape route. CI personnel should determine the route the individual took to get to US lines or checkpoints. Question the individual further on time, distance, and method of travel to determine whether or not the trip was possible during the time stated and with the mode of transportation used. Discrepancies in travel time and distances can be the key to the discovery of an infiltrator with a shallow cover story. By determining what an individual observed enroute, the screener can either check the person's story or pick up intelligence information concerning the enemy forces. Interrogators are well trained in this process and should be called upon for assistance and training.

f. Indicators.

(1) Use the following indicators in an attempt to identify hostile infiltrators. CI personnel look for persons:

(a) Of military age.

(b) Traveling alone or in pairs.

(c) Without ID.

(d) With unusual documents.

(e) Possessing large amounts of money, precious metals, or gems.

(f) Displaying any peculiar activity.

(g) Trying to avoid detection or questioning.

(h) Using enemy methods of operating.

(i) Having a pro-enemy background.

(j) With a suspicious story.

(k) With a family in enemy areas.

(l) With a technical skill or knowledge.

(m) Who have collaborated.

(n) Who violate regulations in enemy areas.

(2) In addition to interrogation, use the following methods of screening EPWs and refugees:

(a) Apprehension lists.

(b) Low-level informants infiltrated into EPW compounds or camps; civilian internee screens or camps; or refugee screens or centers.

(c) Sound equipment placed in suspect-holding areas or cages.

(d) Polygraph examinations.

(e) Specialized identification equipment, for example, metal-trace detection kits.

g. Checkpoints.

(1) This type of CI screening requires CI personnel to prepare apprehension lists and indicators to be used by screening teams. Specialized equipment such as metal detection kits would significantly enhance the screening process. These teams will provide the initial screening and will detain and refer suspects to the Ml control element for detailed 06 or CI interrogation and possible exploitation. Screening teams can be made up of combat troops, MP, CA, intelligence interrogators, and CI agents.

(2) Place checkpoints shown in Figure A-IV-1 at strategic locations, where there is sufficient space for assembling people under guard and for parking vehicles for search and investigation. Set these up as either mobile or static missions. Post local security to protect the checkpoint and post a sufficient amount of personnel to the front and rear to catch anyone attempting to avoid the checkpoint. The preparation needed for static and mobile checkpoints is identical to other screening operations, and the indicators will remain basically the same.

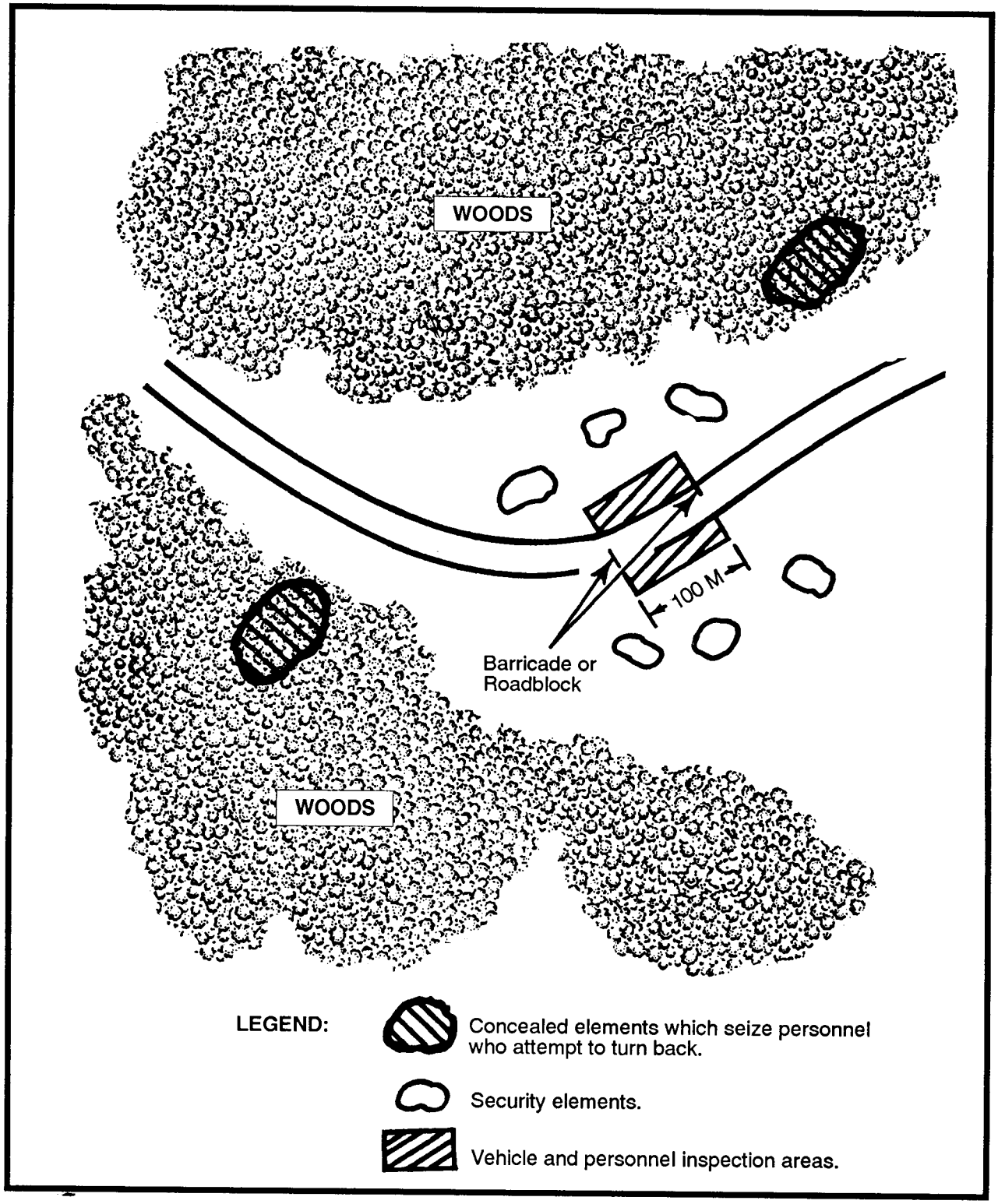

Figure A-IV-1. Example of a checkpoint.

(a) Mobile. Use a mobile checkpoint as a moving system by which the team, either mounted or on foot, briefly selects individuals at random. Locate these checkpoints at various points for periods not to exceed one day.

(b) Static. Static checkpoints are those manned permanently by MP or troops at the entrance to a bridge, town gate, river crossing, or similar strategic point.

A-IV-3. **Cordon and Search.** The purpose for conducting cordon and search operations is to identify and apprehend persons hostile to our efforts and to exploit information gathered.

a. Before conducting a community or area cordon and search operation, CI personnel must coordinate with local officials to solicit their support and cooperation. They must coordinate with the host country area coordination center, if established. If not established, they must coordinate with host country intelligence and police organization to—

(1) Obtain their participation in the operation.

(2) Update existing personalities list (black and gray lists).

(3) Arrange to have insurgent defectors, agents, and other knowledgeable personnel present to identify insurgents and their supporters.

(4) Update all intelligence on the community or area.

b. CI personnel must coordinate with appropriate US and host country CA and PSYOP units. Coordination must also be done with the unit conducting the operation. An essential part of preparing for a cordon and search is an update of all intelligence on the community or area.

c. The senior tactical unit commander will be the individual responsible for the conduct of the operation. That commander will plan, with advice from CI, interrogation, CA, and PSYOP personnel, the cordon which is usually deployed at night, and the search which normally begins at first light.

d. Community operations.

(1) The basic operation is the community cordon and search operation shown in Figure A-IV-2. As the screening element sets up the collection or screening station shown in Figure A-IV-3, the sweep element escorts the residents toward the station, leaving behind one resident to care for family belongings, if required by law.

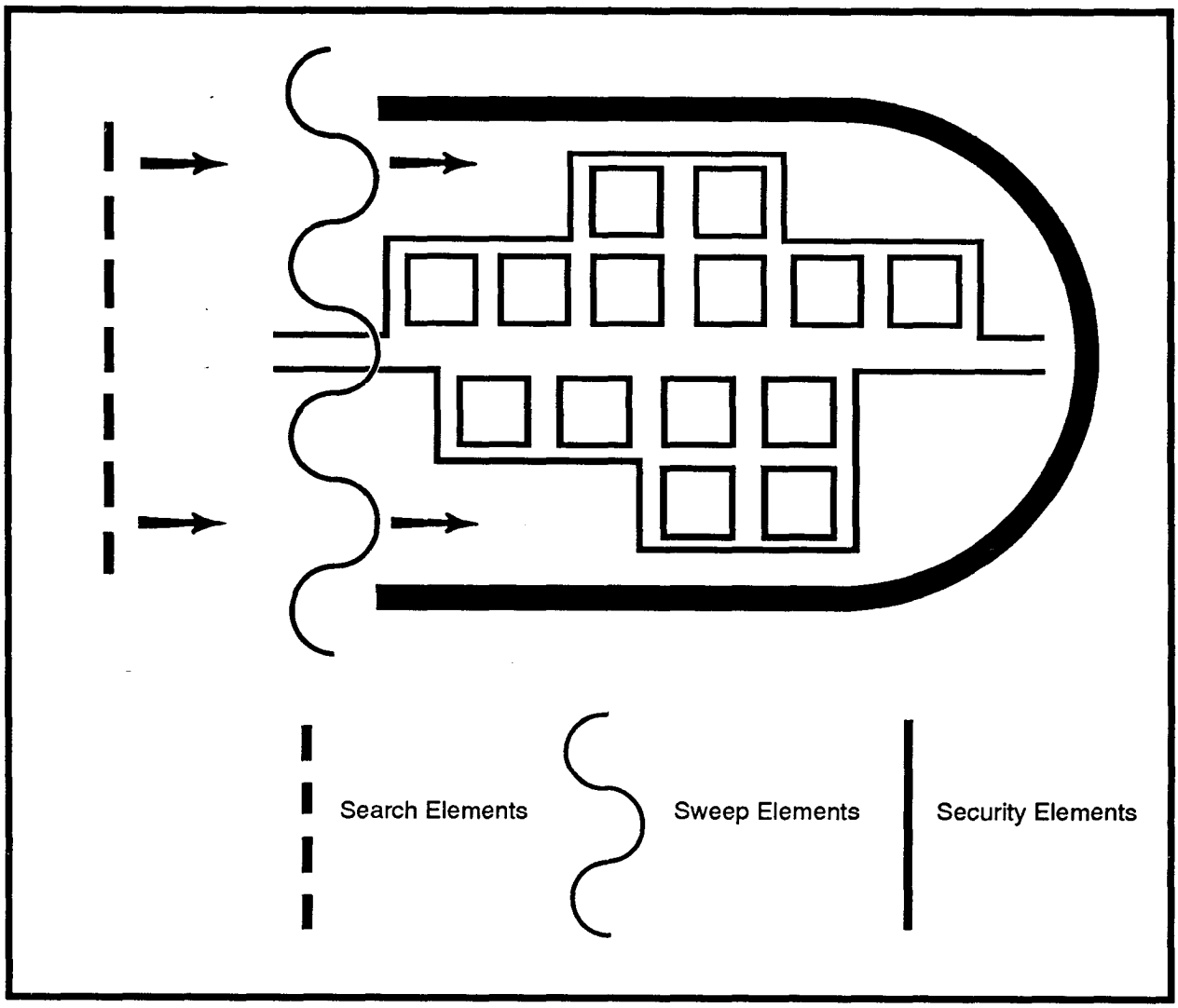

Figure A-IV-2. Example of community cordon and search operations.

(2) The search element follows behind the sweep element searching houses, storage areas, cemeteries and so forth, with dogs and metal detection equipment. CI personnel are searching for evidence of intelligence collection operations to include communications codes or other such paraphernalia. Each search element should include a CI team with an interrogator team as required, which will have a list of persons of CI interest.

(3) In the collection or screening station, bring the residents to the collection area (or holding area) and then systematically lead them to specific screening stations. Enroute to the screening station, search each individual for weapons. Then lead the residents past the mayor or community leaders (enemy defectors or cooperating prisoners who will be hidden from view so that they can uncompromisingly identify any recognizable enemy). These informants will be provided with the means to notify a nearby guard or a screener if they spot an enemy member. Immediately segregate this individual and interrogate by appropriate personnel.

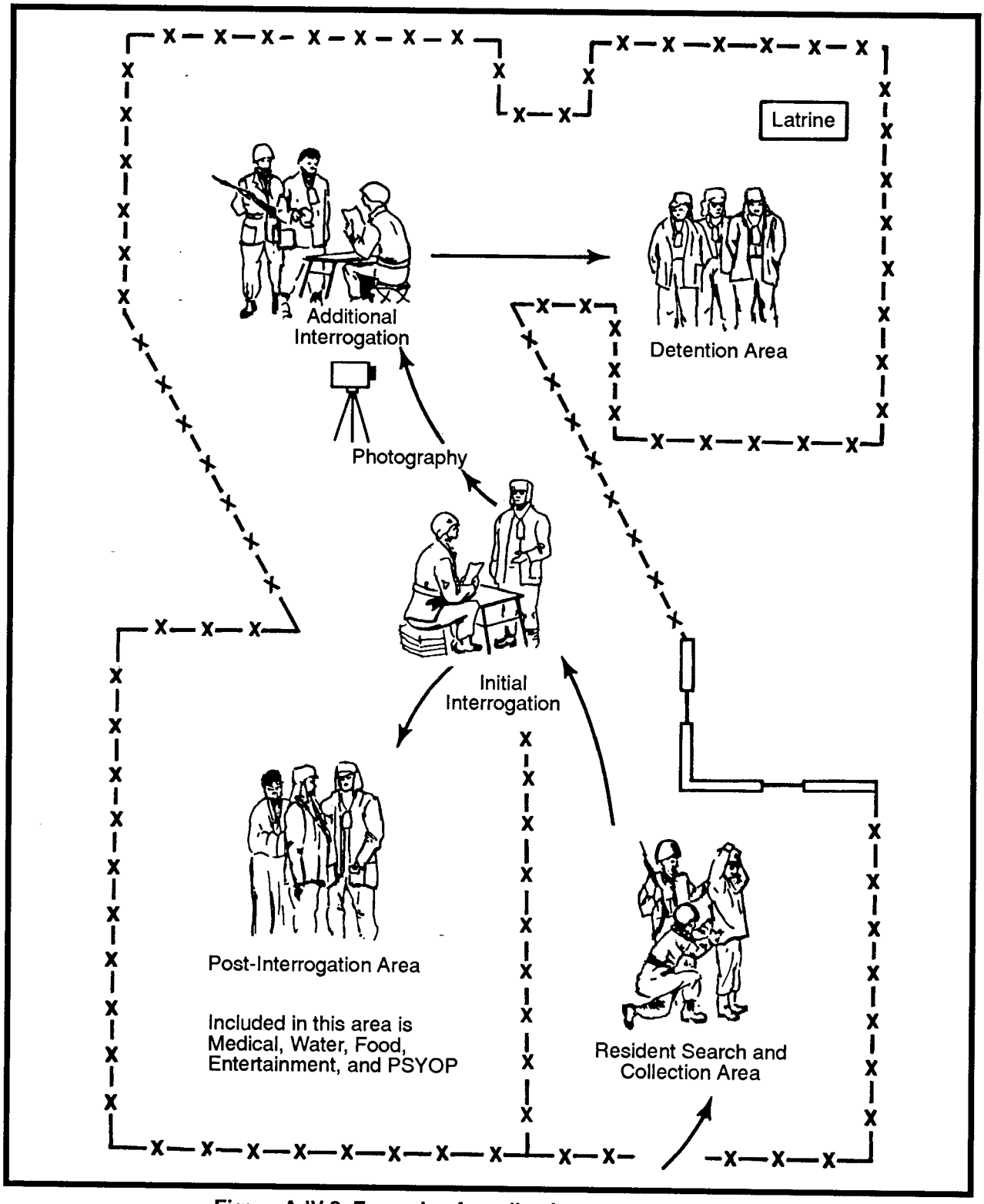

Figure A-IV-3. Example of a collection screening station.

(4) At specific screening stations, ask the residents for identification, check against personalities list (black list), and search for incriminating evidence by electronic equipment.

(5) Move suspected persons on for photographing, further interrogation, or put them in the screening area detention point to be taken back to a base area or area coordination center interrogation facility for detailed interrogation upon completion of the operation.

(6) Pass innocent residents through to the post screening area where they are provided medical assistance and other civic assistance, as well as entertainment and friendly propaganda.

(7) Return any persons caught attempting to escape or break through the cordon immediately to the detention area.

(8) When the operation is terminated, allow all innocent individuals to return to their homes, and remove the enemy suspects under guard for further interrogation. Photograph all members of the community for compilation of a village packet, which will be used in future operations.

e. "Soft" or area operation.

(1) The second type of cordon and search operation is very frequently referred to as the "soft" or area cordon and search. This operation includes the cordoning and searching of a rather vast area (for example, a village area incorporating a number of hamlets, boroughs, town, or villages which are subdivisions of a political area beneath country level).

(2) This type of operation requires a multibattalion military force to cordon off the area; a pooling of all paramilitary, police, CA, and intelligence resources to conduct search and screening; and a formidable logistical backup. This kind of operation extends over a period of days and may take as long as a week or possibly longer.

(3) While screening and search teams systematically go from community to community and screen all residents, military forces sweep the area outside the communities over and over again to seek out anyone avoiding screening. As each resident is screened, CI agents will issue documents testifying to the fact that he was screened and if necessary, allow him restricted travel within the area.

(4) Other population and resource{ control measures are used as well. Such an opportunity may allow the chance to issue new ID cards and photograph all of the area's residents.

(5) As each community screening proceeds, send individuals who were designated for further interrogation to a centralized interrogation center in the cordoned area. Here, CI personnel will work with intelligence interrogation personnel, both US and indigenous, police, and other security service interrogators.

(6) Besides field files and other expedient facilities, a quick reaction force is located at the interrogation center to react immediately to intelligence developed during the interrogations and from informants planted among the detainees.

Section V

PERSONALITIES, ORGANIZATIONS, AND INSTALLATIONS LIST

TO

Appendix A

COUNTER-HUMAN INTELLIGENCE TECHNIQUES AND PROCEDURES

A-V-1. **GeneraI.** The effectiveness of CI operations depends largely on the planning that precedes the operation. Early in the planning process the CI officer on the G2 staff directs the efforts to obtain information on the adversary's intelligence, sabotage, terrorism, and subversion capabilities. Collected information is processed and analyzed, and from it the CI officer formulates a list of CI targets. Section V identifies the criteria for the personalities, organizations, and installations list. CI targets are personalities, organizations, and installations of intelligence or CI interest which must be seized, exploited, or protected.

A-V-2. **Personalities.** These are persons who are a threat to security, whose intentions are unknown, or who can assist the intelligence and CI efforts of the command. Personalities are grouped into these three categories. For ease in identification, a color code indicates the category. Colors currently in use are black, gray, and white and pertain to the three categories in the order listed above.

a. Black list. The black list is an official CI listing of actual or potential enemy collaborators, sympathizers, intelligence suspects, and other persons whose presence menaces the security of the friendly forces. (Joint Pub 1-02) Black list includes—

(1) Known or suspected enemy or hostile espionage agents, saboteurs, terrorists, political figures, and subversive individuals.

(2) Known or suspected leaders and members of hostile paramilitary, partisan, or guerrilla groups.

(3) Political leaders known or suspected to be hostile to the military and political objectives of the US or an allied nation.

(4) Known or suspected officials of enemy governments whose presence in the theater of operations poses a security threat to the US Forces.

(5) Known or suspected enemy collaborators and sympathizers whose presence in the theater of operations poses a security threat to the US Forces.

(6) Known enemy military or civilian personnel who have engaged in intelligence, CI, security, police, or political indoctrination activities among troops or civilians.

(7) Other personalities indicated by the G2 as automatic arrestees. Included in this category may be local political personalities, police chiefs, and heads of significant municipal and national departments or agencies, and tribal or clan leaders.

b. Gray list. The gray list contains the identities and locations of those personalities whose inclinations and attitudes toward the political and military objective to the US are obscure. Regardless of their political inclinations or attitudes, personalities may be listed on gray lists when they are known to possess information or particular skills required by US Forces. These people are the "unknowns." They may be individuals whose political motivations require further exploration before they can be used effectively by US Forces. Examples of individuals who may be included in this category are—

(1) Potential or actual defectors from the hostile cause whose bona fides have not been established.

(2) Individuals who have resisted, or are believed to have resisted, the enemy government and who may be willing to cooperate with US Forces, but whose bona fides have not been established.

(3) Scientists and technicians suspected of having been engaged against their will in enemy research projects of high technology programs.

c. White list. The white list contains the identities and locations of individuals who have been identified as being of intelligence or CI interest and are expected to be able to provide information or assistance in existing or new intelligence Als. They are usually in accordance with, or favorably inclined toward, US policies. Their contributions are based on a voluntary and cooperative attitude. Decisions to place individuals on the white list may be affected by the combat situation, critical need for specialists in scientific fields, and such theater intelligence needs as may be indicated from time to time. Examples of individuals who may be included in this category are—

(1) Former political leaders of a hostile state who were deposed by the hostile political leaders.

(2) Intelligence agents employed by US or allied intelligence agencies.

(3) Key civilians in areas of scientific research, who may include faculty members of universities and staffs of industrial or national research facilities, whose bona fides have been established.

(4) Leaders of religious groups and other humanitarian groups.

(5) Other persons who can materially and significantly aid the political, scientific, and military objectives of the US and whose bona fides have been established.

A-V-3. **Installations.** Installations on the CI targets list are any building, office, or field position that may contain information or material of CI interest or which may pose a threat to the security of the command. Installations of CI interest include—

a. Those that are or were occupied by enemy espionage, sabotage, or subversive agencies or police organizations, including prisons and detention centers.

b. Those occupied by enemy intelligence, CI, security, or paramilitary organizations including operational bases, schools, and training sites.

c. Enemy communication media and signal centers.

d. Nuclear research centers and chemical laboratories.

e. Enemy political administrative HQ.

f. Public utilities and other installations to be taken under early control to prevent sabotage.

g. Production facilities, supply areas, and other installations to be taken under control to prevent support to hostile guerrilla and partisan elements.

h. Embassies and consulates of hostile governments.

A-V-4. **Organizations.** Any group that is a potential threat to the security of the friendly force must be neutralized, rendered ineffective. Groups or organizations which are of concern to CI during tactical operations include—

a. Hostile intelligence, sabotage, subversive, and insurgent organizations.

b. National and local political parties or groups known to have aims, beliefs, or ideologies contrary or in opposition to those of the US.

c. Paramilitary organizations, including students, police, military veterans, and excombatant groups known to be hostile to the US.

d. Hostile sponsored organizations or groups whose objectives are to create dissention and spread unrest among the civilian population in the AO.

A-V-5. **Control Measures.** The CI officer and the G2 need a positive way to keep track of the status of CI targets. Called a target reduction plan, it's a checklist used to ensure targets are seized, exploited, or controlled in a timely manner. The plan is keyed to the scheme of maneuver and lists targets as they are expected to appear. When more targets appear than can be exploited, a priority list is used to denote which target takes priority.

a. Priority one targets represent the greatest threat to the command. They possess the greatest potential source of information or material of intelligence or CI value. Priority one targets must be exploited or neutralized first.

b. Priority two targets are of lesser significance than priority one. They are taken under control after priority one targets have been exploited or neutralized.

c. Priority three targets are of lesser significance than priority one or two. They are to be exploited or neutralized as time and personnel permit.

Section VI

COUNTER-HUMAN INTELLIGENCE ANALYSIS

TO

Appendix A

COUNTER-HUMAN INTELLIGENCE TECHNIQUES AND PROCEDURES

A-VI-1. **General.** C-HUMINT analysis increases in importance with each new US involvement in worldwide operations. Especially in OOTW, C-HUMINT analysis is rapidly becoming a cornerstone upon which commanders base their concepts operations. This section presents information for analysts to develop some of those products that can enhance the probability of successful operations.

a. MDCI analysts, interrogators, and CI agents maintain the C-HUMINT database. Using this database, they produce—

(1) Time event charts.

(2) Association matrices.

(3) Activities matrices.

(4) Link diagrams.

(5) HUMINT communication diagrams.

(6) HUMINT situation overlays.

(7) HUMINT-related portions of the threat assessment.

(8) CI target lists.

b. The analytical techniques used in HUMINT analysis enable the analyst to visualize large amounts of data in graphic form. We emphasize, however, that these analytical techniques are only tools used to arrive at a logical and correct solution to a complex problem; the techniques themselves are not the solution.

c. There are three basic techniques (tools) used as aids in analyzing HUMINT-related problems. These techniques— **time event charting, matrix manipulation, and link diagraming** —used together, are critical to the process of transforming diverse and incomplete bits of seemingly unrelated data into an understandable overview of an exceedingly complex situation.

(1) Time event charting.

(a) The time event chart shown in Figure A-VI-1, is a chronological record of individual or group activities designed to store and display large amounts of information in as little space as possible. This tool is easy to prepare, understand, and use. Symbols used in time event charting are very simple. Analysts use triangles to show the beginning and end of the chart. They also use triangles within the chart to show shifts in method of operation or change in ideology. Rectangles or diamonds are used to indicate significant events or activities.

(b) Analysts can highlight particularly noteworthy or important events by drawing an "X" through the event symbol (rectangle or diamond). Each of these symbols contains a chronological number (event number), date (day, month, and year of event), and may contain a file reference number. The incident description is a very brief explanation of the incident, and may include team size, type of incident or activity, place and method of operation, and duration of incident. Time flow is indicated by arrows.

(c) Analysts also use a variety of symbols such as parallelograms and pentagons, and others, to show different types of events and activities. Using these symbols and brief descriptions, the MDCI analyst can analyze the group's activities, transitions, trends, and operational patterns. Time event charts are excellent briefing aids as well as flexible analytical tools.

(2) Matrix manipulation.

(a) Construction of a matrix is the easiest and simplest way to show relationships between similar or dissimilar associated items. The "items" can be anything relevant to the situation under investigation: persons, events, addressees, organizations, or telephone numbers. During this process, MDCI analysts use matrices to determine "who knows whom" or "who has been where or done what." This results in a clear and concise display which viewers can easily understand simply by Iooking at the matrix.

(b) In general terms, matrices resemble the mileage charts commonly found in a road atlas. Within the category of matrices, there are two types used in investigative analysis— **association matrix** and **activities matrix.**

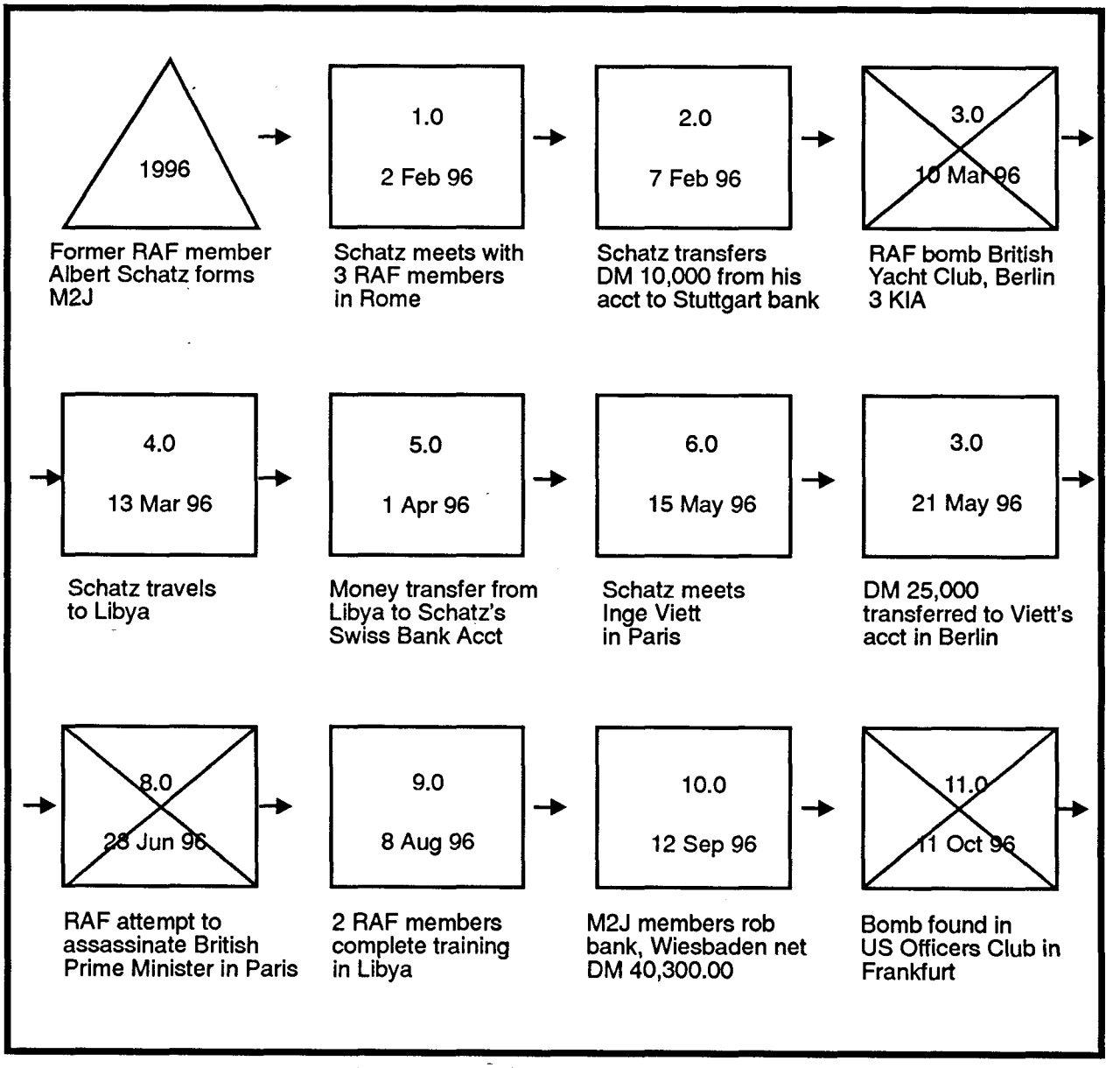

Figure A-VI-1. Sample time event chart.

1 Association matrix. The association matrix is used to show that a relationship between individuals exists. Within the realm of HUMINT analysis, the part of the problem deserving the most analytical effort is the group itself. Analysts examine the group's elements (members) and their relationships with other members, other groups and associated entities, and related events. Analysts can show the connections between key players in any event or activity in an association matrix shown in Figure A-VI-2. It shows associations within a group or similar activity, and is based on the assumption that people involved in a collective activity know one another.

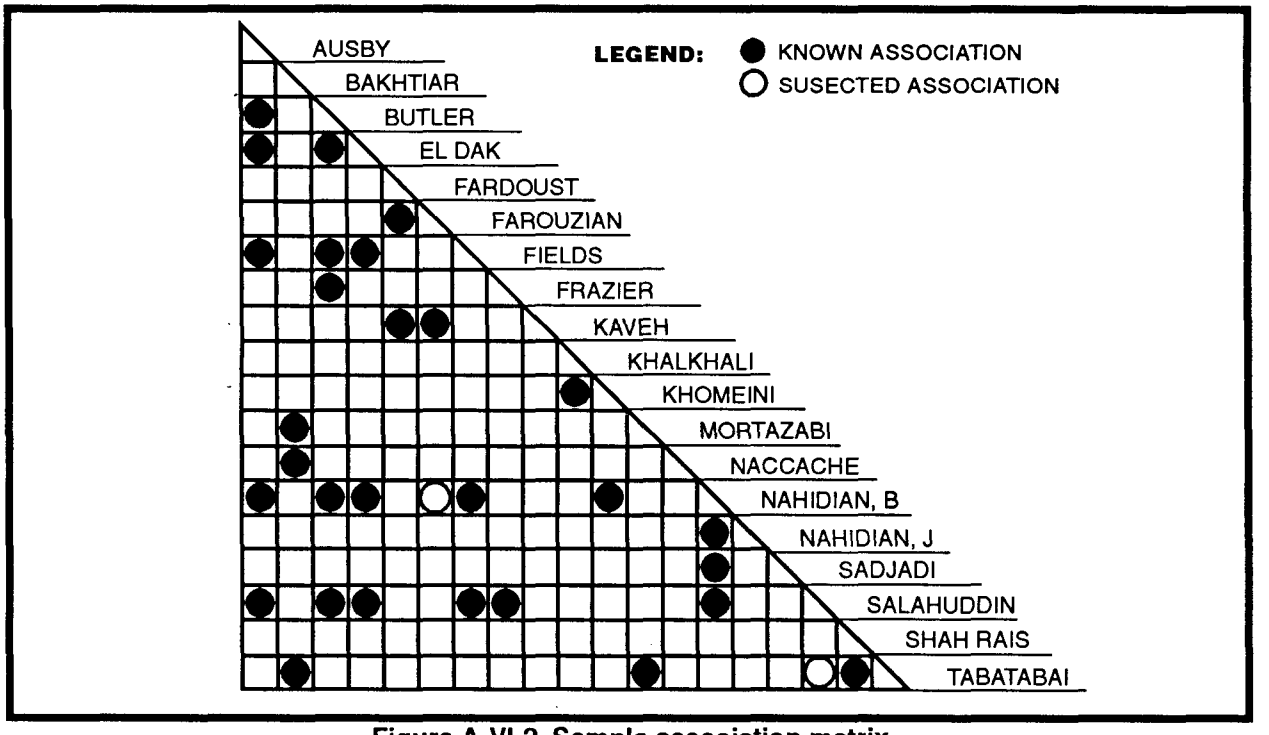

Figure A-VI-2. Sample association matrix.

a This type of matrix is constructed in the form of a right triangle having the same number of rows and columns. Analysts list personalities in exactly the same order along both the rows and columns to ensure that all possible associations are shown correctly. The purpose of the personality matrix is to show who knows whom. Analysts determine a known association by "direct contact" between individuals. They determine direct contact by a number of factors, including face-to-face meetings, confirmed telephonic conversation between known parties, and all members of a particular organizational cell.

NOTE: When a person of interest dies, a diamond is drawn next to his or her name on the matrix.

b MDCI analysts indicate a known association between individuals on the matrix by a dot or filled-in circle. They consider suspected or "weak" associations between persons of interest to be associations which are possible or even probable, but cannot be confirmed using the above criteria. Examples of suspected associations include—

- A known party calling a known telephone number (the analyst knows to whom the telephone number is listed), but cannot determine with certainty who answered the call.
- The analyst can identify one party to a face-to-face meeting, but may be able to only tentatively identify the other party.

(c) Weak or suspected associations on the personality matrix are indicated by an open circle. The rationale for depicting suspected associations is to get as close as possible to an objective analytic solution while staying as close as possible to known or confirmed facts. If analysts can confirm a suspected association, they can make the appropriate adjustment on the personality matrix.

(d) A secondary reason for depicting suspected associations is that it may give the analyst a focus for tasking limited intelligence collection assets to confirm the suspected association. An important point to remember about using the personality matrix: it will show only that relationships exist; not the nature, degree, or frequency of those relationships.

2 Activities matrix. The activities matrix is used to determine connectivity between individuals and any organization, event, entity, address, activity, or anything other than persons. Unlike the association matrix, the activities matrix is constructed in the form of a square or a rectangle as shown in Figure A-VI-3. It does not necessarily have the same number of rows and columns. The analyst can tailor rows or columns to fit the needs of the problem at hand or add them later as the problem expands in scope. The analyst determines the number of rows and columns by the needs of the problem and by the amount of information available.

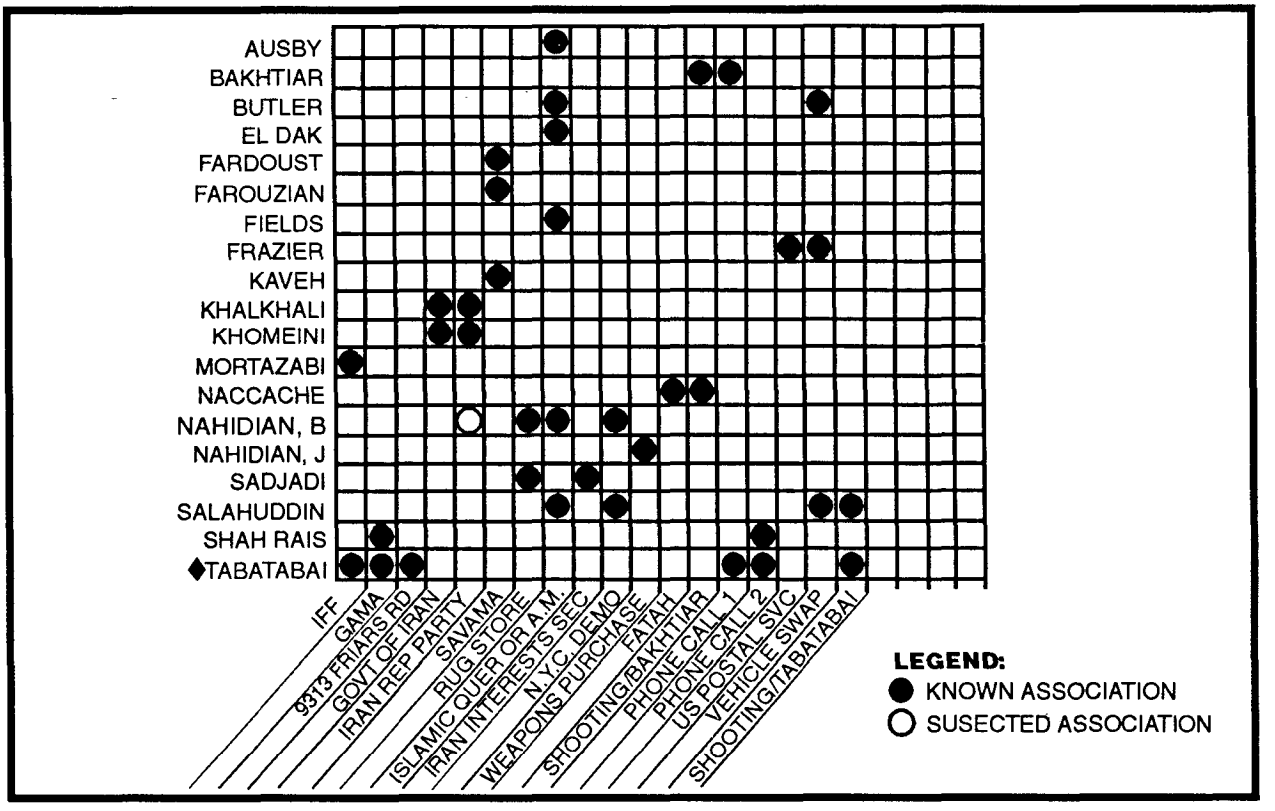

Figure A-VI-3. Sample activities matrix.

a Analysts normally construct this matrix with personalities arranged in a vertical listing on the left side of the matrix; and activities, organizations, events, addresses, or any other common denominator arranged along the bottom of the matrix.

b This matrix can store an incredible amount of information about a particular organization or group, and can build on information developed in the association matrix. Starting with fragmentary information, the activities matrix can reveal an organization's—

- Membership.
- Organizational structure.
- Cell structures and size.
- Communications network.
- Support structure.
- Linkages with other organizations and entities.
- Group activities and operations.
- Organizational and national or international ties.

c As with the association matrix, known association between persons and entities is indicated by a solid circle, and suspected associations by an open circle.

d Analysts use matrices to present briefings, present evidence, or store information in a concise and understandable manner within a database. Matrices augment, but cannot replace, standard reporting procedures or standard database files. Using matrices, the analyst can—

- Pinpoint the optimal targets for further intelligence collection.
- Identify key personalities within an organization.
- Increase the analyst's understanding of an organization and its structure.

NOTE: The graphics involved in constructing-the two types of matrices differ slightly, but the principles are the same.

(3) Link diagraming. The third analytical technique is link diagraming shown in Figure A-VI-4. Analysts use this technique to depict the more complex linkages between a large number of entities, be they persons, events, organizations, or almost anything else. Analysts use link analysis in a variety of complex investigative efforts including criminal investigations, terrorism, analysis, and even medical research. Several regional law enforcement training centers are currently teaching this method as a technique in combatting organized crime. The particular method discussed here is an adaptation especially useful in CI investigative analysis in general and terrorism analysis in particular.

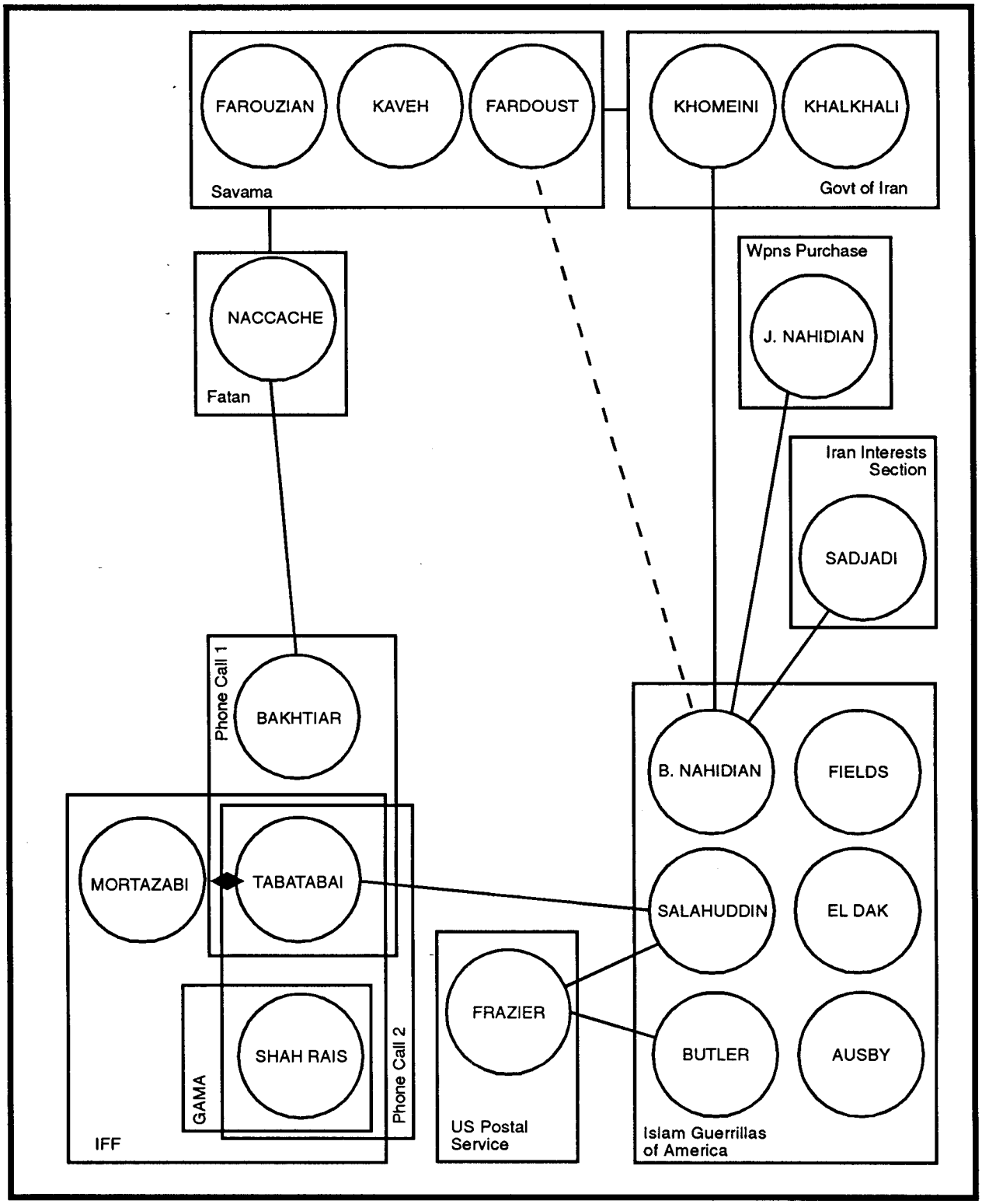

Figure A-VI-4. Sample link diagram.

(a) The difference between matrices and link analysis is roughly the same as the difference between a mileage chart and a road map. The mileage chart shows the connections between cities using numbers to represent travel distances. The map uses symbols that represent cities, locations, and roads to show how two or more locations are linked to each other. Different symbols on the map have different meanings, and it is easy to display or discover the best route between two or more locations as well as identify obstacles such as unpaved roads or bodies of water.

(b) The same is true with link analysis. Different symbols are used to identify different items. Analysts can easily and clearly display obstacles, indirect routes or connections, and suspected connections. In many cases, the viewer can work with and follow the picture easier than the matrix. Link analysis can present information in a manner that ensures clarity.

(c) As with construction of association matrices, certain rules of graphics, symbology, and construction must be followed. Standardization is critical to ensure that everyone constructing, using, or reading a link diagram understands exactly what the diagram depicts. The standard rules follow:

1 Show persons as open circles with the name written inside the circle.

2 Show persons known by more than one name (alias, also known as [AKA]) as overlapping circles with names in each circle.

3 Show deceased persons as above, with a diamond next to the circle representing that person.

4 Show nonpersonal entities (organizations, governments, events, locations) by squares or rectangles.

5 Show linkages or associations by lines: solid for confirmed and dotted for suspected.

6 Show each person or nonpersonal entity only once in a link diagram.

(d) Certain conventions must be followed. For the sake of clarity, analysts arrange circles and squares so that whenever possible, lines of connectivity do not cross. Often, particularly when dealing with a large or especially complex problem, it is difficult to construct a link diagram so that no connecting lines cross. Intersecting lines, however, muddle the drawing and reduce clarity. If lines must cross, show the crossing as a crossing, not as an intersection, in exactly the same manner as on an electrical schematic or diagram.

(e) Link diagrams can show organizations, membership within the organization, action teams or cells, or participants in an event. Since each individual depicted on a link diagram is shown only once, and some individuals may belong to more than one organization or take part in more than one event, squares or rectangles representing nonpersonal entities may overlap.

(f) Construct the appropriate association matrices showing "who knows whom," "who participated in what," "who went where," and "who belongs to what group."

(g) Draw information from the database and intelligence reports, and relationships from the matrices. Group persons into organizations or cells based on information about joint association, activities, or membership. Draw lines representing connections between individuals, organizations, or activities to complete the diagram. You may have to rearrange the diagram to comply with procedural guidelines, such as crossed lines of connectivity. The finished product will clearly display linkages between individuals, organizations, and other groupings.

(h) When you finish the matrices and link diagram, make recommendations about the group's structure. Identify areas for further intelligence collection targeting. Task intelligence assets to confirm suspected linkages and identify key personalities for exploitation or neutralization. The combination of matrix manipulation and the link diagram present, in effect, a graphic depiction of an extremely complex threat situation in a clear and concise picture.

(i) Overlapping organizations.

1 There is more to overlapping organizations than is immediately obvious. At first glance, the overlap indicates only that an individual may belong to more than one organization or has taken part in multiple activities. Further study and analysis would reveal connections between organizations, connections between events, or connections between organizations and events.

2 When, as is often the case, an organization or incident shown in a link diagram contains the names of more than one individual, it is not necessary to draw a solid line between those individuals to indicate connectivity. We assume that individual members of the same group or participants in the same activity know each other, and the connection between them is therefore implied.

(j) A final set of rules for link diagrams concerns connectivity between individuals who are not members of an organization or participants in an activity, but who are somehow connected to the group or activity. Two possibilities exist: The individual knows a member or members of the organization but is not directly connected with the organization itself. The person is somehow connected with the organization or activity but cannot be directly Iinked with any particular member of that organization or activity. In the first case, draw the connectivity line between the circle representing the individual and the circle representing the person within the organization or activity.

(k) If you keep in mind the preceding outline of principles and rules, you can construct a link diagram effectively. Because this is a rather complex form of analytical graphic display to construct, it may prove difficult at first and require a little extra time and effort. The payoff, however, is the powerful impact of the results, which are well worth the extra effort.

Section VII

PERSONNEL SECURITY INVESTIGATIONS

TO

Appendix A

COUNTER-HUMAN INTELLIGENCE TECHNIQUES AND PROCEDURES

A-VII-1. **Personnel Security Investigations.** CI agents conduct PSIs on individuals requiring access to classified information. DIS Manual 20-1-M contains personnel security investigative requirements, types and scope of investigations, and the criteria for each component of a PSI. It also contains the methods and procedures governing the conduct of PSIs. In CONUS, DIS conducts PSIs; and OCONUS, the military services conduct PSIs on behalf of DIS.

a. There are several types of PSIs. Each type provides the individual with a different level of access to classified information. The types of PSIs are national agency checks (NACs), single scope background investigations (SSBIs), and LAA.

(1) NAC. An NAC consists, as a minimum, of a check of the Defense Central Index of Investigations (DCII) and the FBI. The FBI check is a review of files for information of a security nature which is developed during applicant-type investigations. It also includes a technical fingerprint search (classification of SUBJECT's fingerprints and comparison with fingerprints on file). If the fingerprint card is not classifiable, a "name check only" is automatically conducted. Office of Personnel Management, INS, State Department, CIA, and other federal agencies also may be checked, depending on the case. An NAC is the minimum investigative requirement for a final SECRET clearance for military personnel. It may be used as a basis for an interim TOP SECRET clearance based on simultaneous submission of a request for a background investigation.

(2) SSBI. An SSBI consists of a records review NAC, interviews with sources of information, and a subject interview; the subject interview being the principal component. The SSBI covers the most recent 10 years of an individual's life or 18th birthday, whichever is shorter, provided the last two years are covered. No investigation is made for the period before the individual's 16th birthday. The SSBI includes local agency checks, interviews of developed character references, employment references with employment records checks, education records checks and interviews, interviews of neighbors at previous residences, credit checks, citizenship verification, plus selected follow-up interviews as required to resolve unfavorable or questionable information. An SSBI is the minimum investigative requirement for granting a final TOP SECRET security clearance or for participation in certain special programs.

(3) LAA. An LAA is the formal authority granted to non-US citizens to have access to specifically prescribed and limited US classified defense information and materials. In each case, an investigation equivalent to the SSBI in scope must be completed with favorable results. A polygraph may be used to compensate for those portions of the SSBI which cannot be accomplished due to geographic or procedural limitations. An LAA may remain in effect for a maximum of five years before reinvestigation.

b. DIS Manual 20-1-M contains a full explanation of PSI requirements and criteria.

A-VII-2. **PSI Reference Interview.** Before conducting a PSI Reference (Source) Interview, the CI agent must carefully examine all available background information on the case without exceeding the agent's standing investigative authority, which allows checks of sources only when identity or reliability is questioned. The SUBJECT of the investigation may have submitted a DD Form 398 which is often the initial source of leads. It may indicate the relationship between the listed references and the subject. It may also assist in creating a mental picture of the SUBJECT—an invaluable aid in formulating a line of questioning for an interview.

a. Source interviews may be tasked by some form of lead sheet, which normally contains limited background information. Leads may also be developed through previous investigative activity. Unit files, local and Federal law enforcement agency files, telephone books, and city directories are all sources of information on both the SUBJECT and potential sources. It is desirable and necessary in critical cases, where the credibility of an interviewee is questionable, to learn something about the Source. A telephone call to arrange an appointment with a prospective Source is a courtesy that is often helpful to the investigator. The final preparatory step is to form a tentative plan for questioning the Source.

b. The approach to a PSI Reference (Source) Interview is simply an application of the social code of polite behavior, together with certain investigative requirements. The CI agent must—

(1) Determine that the right person has been contacted, using the full name of the interviewee or Source to prevent any possibility of error.

(2) Identify the SUBJECT of the investigation and find out if the Source is or was acquainted with the SUBJECT.

(3) Present credentials to the Source for inspection, even if the individual was previously contacted by telephone.

(4) Ensure, to the extent possible, that the interview will not be interrupted or overheard. Emphasize the US Army policy limiting dissemination of details of an investigation.

(5) Explain the purpose of the interview to the Source. The CI agent should emphasize the importance the Source's knowledge may have to the investigation. Some people are inclined to look with suspicion at investigators and are reluctant to give information. A patient explanation of the purpose of the interview, and the important part the Source's cooperation may play, may be sufficient to allay this general suspicion and forestall any reluctance to provide information.

(6) Inform the Source that the interview and the matters discussed are regarded by the US Army as official US Army business and should not be discussed with other persons, especially the SUBJECT of the investigation.

(7) Advise the Source of the Privacy Act of 1974. Ask the Source if there are any objections to the release of the interviewee's name as the source of the information. This advisement should be given at the termination of the interview to both US citizens and resident aliens, unless Source raised the question of disclosure earlier in the interview. OCONUS interviews of foreign nationals, who are not US resident aliens, do not require a Privacy Act advisement.

(8) Establish rapport with the Source before beginning the interview. Proper rapport creates a mutual understanding between the parties of the interview. Professional appearance, a pleasant voice, a courteous demeanor, and a confident manner are all important. The burden for maintaining rapport throughout an interview rests with the CI agent. An interview normally takes place in the Source's home or place of work, where the individual is under no official compulsion to furnish the information sought. Topics of mutual interest should be used to help establish rapport, but caution must be exercised to keep the interview from becoming a casual conversation.

c. Once a Source is willing to cooperate, begin the questioning to establish the period of association with the SUBJECT and the extent of personal knowledge of the SUBJECT.

(1) The period of association consists of—

(a) When the Source and the SUBJECT first met and under what circumstances.

(b) When they last met and under what circumstances.

(c) All periods of association.

(d) Types of association, such as friends, coworkers, or both.

(e) Frequency of contact, for both social and professional association.

(f) Breaks in contact for periods of 30 days or more.

(g) Whether there has been any form of communication between them since their last contact.

(2) This information also aids in developing systematic questions on the loyalty, integrity, discretion, and moral character of the SUBJECT. It is important that the CI agent lay a framework for the interview, through a thorough understanding of the association between the Source and the SUBJECT. In addition, the association area may disclose leads which may be exploited later.

d. The CI agent must exploit all aspects of the SUBJECT's background. The CI agent must be constantly alert for leads to other persons not listed by the SUBJECT as references. If the Source is or was an employee or coworker of the SUBJECT, attention should focus on the efficiency, initiative, and ability of the SUBJECT to get along with fellow workers and subordinates and on the SUBJECT's honesty, reliability, and general character. If the Source is or was a neighbor of the SUBJECT, the CI agent should discuss the SUBJECT's general reputation, family, leisure time activities, morals, and personal habits. Concentration on some points does not imply exclusion of others.

e. The CI agent must seek information which will assist in establishing the SUBJECTS loyalty, trustworthiness, and suitability. Figure A-VII-1 shows the general area of interest for an interview and a basis for discussion.

f. Avoid questions concerning religious beliefs, racial matters, politics, labor affiliations, or personal and domestic matters, unless absolutely essential to the investigation; such questions not relevant to the purpose of the interview constitute unnecessary and unwarranted invasion of the SUBJECT's privacy.

g. The CI agent, as a representative of MI, should be professional in manner and efficient in the execution of duty. The agent must be receptive and flexible.

(1) The agent should dress either in civilian clothes or uniform according to assigned duty and mission. The agent pinpoints specific information desired and avoids general questions. When the Source states, for example, that the SUBJECT is an indiscreet person, request that the Source cite specific examples to support this opinion. If the Source claims the SUBJECT is a drunkard, the individual's definition of the term should be clearly established and specific details obtained.

(2) Analyze each phase of the SUBJECT's background point-by-point.

(3) If the Source presents information in a haphazard manner, the CI agent should guide the discussion into a logical pattern.

A-VII-3. **PSI SUBJECT Interview.**

a. CI agents conduct SUBJECT Interviews when tasked by DIS in the lead sheet.

b. If the SUBJECT is suspected of violating the law, the CI agent must advise the individual of rights under the provisions of the Fifth Amendment to the US Constitution or Article 31, UCMJ, as appropriate. The CI agent must remember that the SUBJECT has the right to legal advice at any time before, during, or after the interview. Note that there are no noncustodial interviews involving a military member according to Article 31, UCMJ.

(1) Birth.	SUBJECT's date and place of birth.
(2) Education.	Names and addresses of institutions, dates of attendance, academic records and degrees received.
(3) Employment.	Names and addresses of employers and dates of employment, names of immediate superiors and coworkers, nature of duties, quality of performance, and reason for termination.
(4) Technical skills.	Education and circumstances of development.
(5) Interests.	Hobbies and avocations.
(6) Foreign activity.	Foreign countries traveled to for personal purposes; friends and relatives who reside in a foreign country, foreign friends, foreign relatives, foreign associates, business or financial interests in foreign countries, correspondence with or visits from persons residing in foreign countries, contact with foreign official representatives or embassies and membership in foreign organizations.
(7) Mental and emotional stability.	General alertness, natural inclination, and idiosyncrasies. Treatment for mental or emotional disorders.
(8) Moral character.	Personal habits, particularly virtues and faults, illegal use of narcotics, and excessive consumption of alcohol.
(9) Loyalty.	Belief in and adherence to the US Constitutional form of government and to the laws of the nation. Reaction to ideologies which are hostile to those of the US Constitutional form of government.
(10) Integrity.	Uprightness of moral character and strength of convictions. Honesty.
(11) Discretion.	Speech and behavior, judgment, and self-control. Respectful of property.
(12) Reputation.	Social and professional.

Figure A-VII-1. Areas of interest for an interview.

(13) Records.	Adverse involvement with law enforcement authorities, both civilian and military. Receipt of courts-martial or nonjudicial punishment.
(14) Finances.	Financial stability and reliability. Evidence of excessive debt or credit problems. Credit bureaus. Evidence of living beyond ones means.
(15) Family background.	Origin of parents, relatives abroad, residences, and citizenship.
(16) Association.	Friends, business or other associates, and favorite haunts.
(17) Organizations.	Membership, active participation, position, professional societies, character of organization, financial contributions, and awareness of aims of organization.
(18) Leads.	Names and addresses of persons acquainted with various phases of the SUBJECT's background and sources of information not listed by subject as references.
(19) Recommendations. (PSIs and as required)	Interviewee's overall opinion of the SUBJECT's qualifications for a position of trust and responsibility. Stress that the recommendation is based on the period of association or a prior period of association, if there is a break in contact between the Source and the SUBJECT.

Figure A-VII-1. Areas of interest for an interview (continued).

c. The CI agent should not raise questions concerning religious beliefs, racial matters, politics, labor affiliations, or personal and domestic matters-unless directly related to the investigation. The CI agent should phrase and time such questions so as to clearly establish the fact that they are relevant to the investigation.

d. To prepare for a SUBJECT Interview, the CI agent—

(1) Contacts the SUBJECT and informs the individual of the reason for the interview. In most cases, the matters to be discussed will not come as a surprise to the SUBJECT. The CI agent tells the SUBJECT that the interview gives the individual an opportunity to explain, refute, or mitigate, questionable or misleading information, and to provide information not otherwise obtainable. If the SUBJECT is willing to be interviewed, the CI agent arranges the time, date, and place for the interview. If the SUBJECT refuses to be interviewed or to answer questions, an official record should be made of the refusal. Provide a brief advisement to the SUBJECT that failure to provide information may adversely affect the processing of the SUBJECT's security clearance.

(2) Gathers all lead information before the interview. Carefully reviews preplanned questions for each interview so that only information specifically authorized by the control office is released to the SUBJECT during the interview.

(3) Ensures that the SUBJECT understands that upon request, and if the individual is called to appear before afield board of inquiry or a civilian security hearing board, the SUBJECT will be provided a copy of any statement provided during the interview. However, the restrictions in AR 380-5 on the release of classified information apply.

(4) Ensures the SUBJECT's copy will not bear a protective marking but will contain a statement substantially as follows: "A copy of (describe) is furnished at your request. The official copies of this document will be protected to safeguard your confidence and will be used for official purposes only."

e. In accordance with the Privacy Act of 1974, whenever a CI agent interviews a SUBJECT, the agent must give the SUBJECT a four-point Privacy Act Advisement. In cases where an advisement of rights is required, the CI agent should provide the SUBJECT with the Privacy Act Advisement statement before the SUBJECT is advised of individual rights under Article 31, UCMJ, or the Fifth Amendment to the US Constitution.

(1) The CI agent should provide the SUBJECT with two copies of the advisement statement. One copy is for the individual's retention, if desired. The CI agent will request the SUBJECT sign the other copy and return it. Privacy Act of 1974 statements are retained but not attached as part of the report.

(2) DIS Manual 20-1-M covers Privacy Act Advisement procedures during the conduct of a PSI under the control of DIS.

(3) The CI agent will verbally inform the SUBJECT that the Privacy Act of 1974 requires that each individual asked to provide personal information be advised of the following four points:

(a) Authority by which the information is being collected.

(b) Principal purpose for which the information will be used.

(c) Routine uses of the information.

(d) Voluntary nature of disclosing information.

(4) Before highlighting the four points, the CI agent should allow sufficient time for the SUBJECT to read the advisement statement.

(5) After highlighting the four points, ask the individual to sign one copy before beginning the interview.

f. During conduct of SUBJECT Interview, the SUBJECT perceives the CI agent as being a representative of the US Army. As such, the SUBJECT will regard the CI agent's every statement,

question, or contact as part of the official proceeding, whether so intended or not. During the interview, the CI agent will—

(1) Make no off-the-record or unofficial remarks in the interview, nor any promises or commitments to the SUBJECT which are beyond the CI agent's legal authority to fulfill.

(2) Avoid statements or representations which may be construed as opinion or advice to the SUBJECT about past, present, or future actions. CI agents should not argue with the SUBJECT or express personal viewpoints on any matter.

(3) Obtain permission from the SUBJECT if a tape or other recorder is to be used during the interview. DIS Manual 20-1-M does not require the use of a tape or other recording device. Take the following actions in the sequence listed. If not recording, omit portions that pertain to the recorder.

(a) Dictate identifying data into a tape recorder before the SUBJECT's arrival. Turn off the machine.

(b) Visually identify the SUBJECT; identify yourself and present credentials; and positively identify the SUBJECT through the use of a pictured ID card, recording all pertinent information from the ID card.

(c) Explain the general purpose and confidential nature of the interview.

(d) Obtain permission to record the interview. Explain that it will facilitate the preparation of a written transcript of the interview, which the SUBJECT will have an opportunity to review, correct, and sign under oath.

(e) Turn on the tape recorder. If the SUBJECT objects to the tape recorder, do not use it. Proceed, but take notes as accurately as possible, while maintaining close attention to the SUBJECT's verbal answers and physical reactions. A tape recording is an administrative convenience, but not having one will not unduly hamper taking the sworn statement and preparing the report.

(f) Administer a full explanation of rights (if required). Request the SUBJECT read and sign DA Form 3881 to acknowledge receipt of the explanation of rights; and to record the individual's decision to exercise or waive the right to remain silent and to consult counsel. If the individual exercises his or her right to silence or to consult counsel, the interview should terminate at this point.

(g) Advise the SUBJECT of the provisions of the Privacy Act of 1974. The CI agent will request the SUBJECT complete the Privacy Act of 1974 Advisement Statement.

(h) Explain to the SUBJECT the DA policy allowing SUBJECTS of investigations every reasonable opportunity to explain, refute, or mitigate information which is developed during the course of an investigation. Furthermore, explain that this is the individual's opportunity to provide whatever information the SUBJECT feels appropriate.

(i) Though not required by DIS Manual 20-1-M, the CI agent may administer the oath of truthfulness to the SUBJECT, following the explanation and acknowledgment of legal rights, but before asking any questions. An appropriate oath is: “Do you affirm that the statements you are about to make are the truth, the whole truth, and nothing but the truth?” Additional remarks such as “So help you God” are unnecessary and may be offensive. If the SUBJECT refuses to take an oath, ask why, then proceed.

(j) Ask the SUBJECT to state his or her name, rank, SSN, DPOB, unit of assignment, duty position, and residence address for the record.

(k) Conduct the interview using the questions from DIS Manual 20-1-M that cover the appropriate topics and prepared questions designed to elicit narrative answers. These prepared questions are only a guide and are not intended to be the only questions asked. The CI agent must fully develop all information provided by the SUBJECT. Record and report all answers accurately.

(1) Make arrangements for the SUBJECT to review and sign a typewritten sworn statement, before ending the interview.

(m) Thank the SUBJECT for cooperating and terminate the interview.

Section VIII

COUNTERINTELLIGENCE INVESTIGATIONS

TO

Appendix A

COUNTER-HUMAN INTELLIGENCE TECHNIQUES AND PROCEDURES

A-VIII-1. **CI Investigations.** CIinvestigations are conducted when sabotage, espionage, spying, treason, sedition, or subversive activity is suspected or alleged. An investigation is initiated by a SAEDA report being submitted and a case being opened by the SCO and ACCO. The primary purpose of each investigation is to identify, neutralize, and exploit information of such a nature, form, and reliability, that may determine the extent and nature of action, if any, necessary to counteract the threat and enhance security.

a. The ACCO and individual SCOs control and direct investigations under the provisions of AR 381-20 and other applicable regulations.

b. The initial objective of investigations involving national security crimes is to determine the nature and extent of damage to national security. Our intent is to develop information of sufficient value to permit its use in the appropriate civil or military court or to initiate CE procedures. However, we should not limit such investigations to the production of evidence. The investigative reports should include all relevant and material information.

c. CI agents conducting investigations must have a thorough understanding of the objectives and operations of foreign espionage, sabotage, and subversive organizations.

d. Investigations are generally incident investigations concerning acts or activities which are committed by, or involve, known or unknown persons or groups of persons. An incident case can involve one or several of the national security crimes: sabotage, espionage, spying, treason, sedition, or subversion. The definitions used in this appendix focus on elements of a crime as an aid to CI personnel in investigations.

A-VIII-2. **Sabotage.** Sabotage is defined as an act, the intent of which is to damage the national defense structure. Intent in the sabotage statute means knowing that the result is practically certain to follow, regardless of any desire, purpose, or motive to achieve the result.

a. Because the first indication of sabotage normally will be the discovery of the injury, destruction, or defective production, most sabotage investigations involve an unknown person or persons.

b. We expect acts of sabotage, both in overseas AOs and in CONUS, to increase significantly in wartime. Sabotage is a particularly effective weapon of guerrilla and partisan groups, operating against logistic and communications installations in occupied hostile areas, and during insurgences. Trained saboteurs sponsored by hostile guerrilla, insurgent, or intelligence organizations may commit acts of sabotage. Individuals operating independently and motivated by revenge, hate, spite, or greed may also conduct sabotage. In internal defense or limited war situations where guerrilla forces are active, we must be careful to distinguish among those acts involving clandestine enemy agents, armed enemy units, or dissatisfied friendly personnel.

c. Normally, we categorize sabotage or suspected sabotage according to the means employed. The traditional types of sabotage are incendiary, explosive, and mechanical. In the future, nuclear and radiological, biological, chemical, magnetic, and electromagnetic means of sabotage will pose an even greater threat to military operations. FM 19-20 discusses the materials and devices used in these types of sabotage.

d. The US Army CIDC will assume the investigative lead for actual or suspected sabotage. The jurisdiction of CI elements is limited to the CI aspects of known or suspected foreign-directed sabotage. CI elements monitor the CIDC investigation and attempt to ascertain the existence of hostile, enemy, or foreign government involvement or the intent of the sabotage. CI elements do not conduct their own separate investigation unless hostile or foreign government involvement is evident or suspected.

e. When CIDC determines that the saboteur is operating on behalf of a foreign power, national security objectives will take precedence over criminal objectives. In this case, CI takes the investigative lead. In situations where CIDC support is not available (such as OOTW), CI elements will conduct the investigation.

f. Sabotage investigations require immediate action. The possibility exists that the saboteur may still be near the scene, or that other military targets may require immediate or additional security protection to avoid or limit further damage. We must preserve and analyze the incident scene before evidence is altered or destroyed.

g. The investigation must proceed with objective and logical thoroughness. The standard investigative interrogatives apply:

(1) Who. Determine a list of probable suspects and establish a list of persons who witnessed or know about the act.

(2) What. Determine what military target was sabotaged and the degree of damage to the target (both monetary and operational).

(3) When. Establish the exact time when the act of sabotage was initiated and when it was discovered; confirm from as many sources as possible.

(4) Where. Determine the precise location of the target and its relation to surrounding activities.

(5) Why. Establish all possibIe reasons for the sabotage act through the investigation of suspects determined to have had motive, ability, and opportunity to accomplish the act.

(6) How. Establish the type of sabotage (such as incendiary, explosive, chemical) and determine the procedures and materials employed through investigation and technical examination and analysis.

h. Destruction of government property. When destruction of government property is involved, CIDC will initially investigate the incident. Upon determination of intent to sabotage, CI and CIDC personnel may conduct a joint investigation of the incident. CIDC will normally retain the investigative lead.

i. An outline of possible investigative actions which may be used to investigate alleged or suspected sabotage incidents follows:

(1) Obtain and analyze the details surrounding the initial reporting of the incident to the CIDC unit. Establish the identity of the person reporting the incident and the reasons for doing so. Determine the facts connected with the reported discovery of the sabotage and examine them for possible discrepancies.

(2) Examine the incident scene as quickly as possible. The CI agent will attempt to reach the scene before possible sources have dispersed and evidence has been disturbed.

(a) The CI agent helps MP personnel protect the scene from disruption. The MP will remove all unauthorized persons from the area, rope off the area as necessary, and post guards to deny entrance and prevent anything from being removed.

(b) Although CI agents should help MP investigators at the crime scene, they should not interfere with the crime scene investigation.

(c) The CI agent may help CIDC personnel process the crime scene, to include locating all possible sources for questioning. CI keeps sources separated only in the sense that CI identifies to the MP or CIDC which ones should be separated. The physical act of separating is an MP or CIDC job.

(3) Preserve the incident scene by taking notes, making detailed sketches, and taking pictures. Arrange for technical experts to help search the scene and collect and preserve physical evidence and obtain all possible clues. Arson specialists, explosives experts, or other types of technicians may be required. Take steps to prevent further damage to the target and to safeguard classified information or material.

(4) Interview sources and obtain sworn statements as soon as possible to reduce the possibility of forgetting details or comparing stories.

(5) Determine the necessary files to be checked. These will be based on examination of the incident scene and by source interviews. CI conducts such action only in coordination with

CIDC. CIDC has the crime scene expertise and responsibility; CI has the modus operandi (MO) expertise to identify to the CIDC.

(a) Files of particular importance may include—

1 Friendly unit MO files.

2 Partisan, guerrilla, or insurgent activity files.

3 Local police files on arsonists.

4 Local police MO files.

5 Foreign intelligence agency MO files.

6 Terrorist MO files.

7 Provost marshal files.

(b) Files checks should include background information on sources and the person or persons who discovered or reported the sabotage.

j. Study all available information such as evidence, technical and laboratory reports, statements of sources, and information from informants in preparation for interrogation of suspects. FM 19-20 contains investigative guidance particularly applicable to the investigation of incendiary sabotage.

A-VIII-3. **Espionage.** Espionage, as defined in Article 106a, UCMJ, and Title 18, US Code, is the act, either directly or indirectly, of obtaining, delivering, transmitting, communicating, or receiving information in respect to national defense with the intent or reason to believe that the information may be used to the injury of the US or to the advantage of any foreign nation. The offense of espionage applies in time of peace or war. There are five elements of espionage. They are contact or communication, collection, tradecraft, reward or motive, and travel. Any or all of these elements are identifiable in counterespionage investigations. If agents recognize the type of information they are trying to collect and analyze data in light of the elements, they have a better understanding of the case and can plan more appropriately.

a. Examples of the elements of espionage are that:

(1) The accused communicated, delivered, or transmitted any document, writing, code book, signal book, sketch, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense.

(2) This matter was communicated, delivered, or transmitted to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the US, or to any representative, officer, agent, employee, subject or citizen thereof, either directly or indirectly.

(3) The accused did so with the intent or reason to believe that such matter would be used to the injury of the US or to the advantage of a foreign nation.

b. Article 106a, UCMJ, further specifies that the punishment for espionage shall be as a court-martial may direct, except that if the accused is found guilty of an offense that directly concerns nuclear weaponry, military spacecraft or satellites, early warning systems, or other means of defense or retaliation against large scale attack, war plans, COMINT or cryptographic information, or any other major weapon system or major element of defense strategy, the accused shall be punished by death or such other punishment as a court-martial may direct.

c. Most espionage investigations originate from reports of incidents involving unknown individuals or allegations regarding known perpetrators. CI agents also conduct investigations of incidents where the crime of espionage has not been formally established, but is only suspected (the theft of classified documents or material). Leads in espionage investigations may originate from a wide variety of sources, including—

(1) Reports from sensitive sources.

(2) Reports from other intelligence, security, and law enforcement agencies.

(3) Evidence of espionage discovered during inspections and surveys of classified document handling and storage procedures.

(4) Reports submitted by military and civilian personnel in accordance with AR 381-12.

(5) Evidence of espionage discovered during screening of refugees, line crossers, displaced persons, civilian internees, EPWs, defectors, and similar groups, in areas of armed conflict.

(6) Information developed during the course of routine PSIs.

d. No single set of investigative procedures is applicable to the conduct of espionage investigations. Espionage is made up of many different elements, and espionage investigations are not always aimed at the arrest and prosecution of the offender. Prosecution of espionage cases may be deferred to the Department of Justice (CONUS) or to the host country (OCONUS). CI agents responsible for such an investigation must have a thorough and up-to-date knowledge of espionage and counterespionage methods and procedures as discussed in FM 34-5 (S).

e. In espionage cases, use any or all of the investigative techniques and tools described in this manual and FM 34-5 (S).

(1) Determine what specific techniques to use on a case-by-case basis.

(2) Get the proper authorization to use investigative techniques.

(3) Conduct the investigation in accordance with current laws and regulations.

f. Records examinations may break the cover story of an espionage suspect. CI agents may use properly authorized physical or technical surveillance to obtain leads or evidence. They may use confidential or sensitive sources or undercover operations to locate and identify suspects. Investigative photography may provide evidence of an attempt to transmit national defense information to a foreign nation.

A-VIII-4. **Spying.** The crime of spying, is defined in Article 106, UCMJ. Spying is strictly limited to a wartime military situation. This is governed by international law, particularly, the Geneva Conventions. Five basic elements are required to constitute the crime of spying:

a. It occurs only during time of war.

b. It is committed within a US military AO.

c. The accused must be caught while seeking information to communicate to the enemy.

d. The accused must have the intent of passing information to the enemy.

e. The accused must have been acting in a clandestine manner.

A-VIII-5. **Treason.** The abuse of treason laws in British legal history led the framers of the US Constitution to include a limiting definition of treason. Article 3, Section III, of the US Constitution also imposes qualifications regarding the conviction of an individual for treason: "No person shall be convicted of treason unless on the testimony of two sources to the same overt actor on confession in open court."

a. Investigations in which treason is suspected or alleged are rare. Historically, most cases occur during wartime, or upon the conclusion of hostilities.

b. Allegations of treason may originate with liberated prisoners of war, interned US civilians, examination of captured enemy records, or interrogation of enemy military and civilian personnel.

c. Federal courts have recognized two distinct types of treason: levying war and aiding and comfort. Investigations will be conducted with a view toward establishing the elements of the particular type of treason.

(1) The elements of levying war treason are the—

(a) Accused owed allegiance to the US.

(b) Accused organized a body of personnel into a military force.

(c) Accused equipped these personnel with arms.

d) Accused made war or military movement with intent to overthrow the government. Levying war treason has not occurred frequently in American history.

(2) Aiding and comfort treason applies to persons with dual citizenship in a wartime situation. The elements of aiding and comfort treason are the—

(a) Accused owed allegiance to the US.

(b) War was formally declared by Congress.

(c) Accused gave aid and comfort to the enemy.

(d) Accused gave such aid and comfort while adhering to the enemy's cause.

d. Records examination, interviews, and interrogations normally are the principal investigative techniques employed in treason investigations. The CI agent pays particular attention to the legal requirements governing the collection and preservation of evidence, especially the taking of statements from sources and suspects.

e. In many cases, the CI agent needs to consult regularly with legal authorities to ensure that the elements of proof are adequately established and that all applicable legal conditions and restrictions are met.

A-VIII-6. **Aiding the Enemy.** Investigations conducted by CI agents to prove or disprove charges brought against an individual under Article 104, UCMJ, may sometimes be treated as treason cases.

a. Article 104, UCMJ, makes five distinct activities criminal. They are—

(1) Aiding the enemy with arms, ammunition, supplies, money, or other things.

(2) Attempting to aid the enemy by performing an overt act with intent to aid the enemy with certain arms, ammunition, supplies, money, or other things.

(3) Without proper authority, harboring or protecting the enemy.

(4) Without proper authority, giving intelligence to the enemy.

(5) Without proper authority, communicating, corresponding, or holding intercourse with the enemy, either directly or indirectly.

b. CI agent personnel must prove that one or more of the prohibited acts occurred. The word "enemy" includes organized forces in time of war, any hostile body that our forces may be opposing, and includes civilians as well as members of military organizations. It is not restricted to enemy government personnel or members of its armed forces. "Enemy" included Communist forces in Vietnam and Korea.

A-VIII-7. **Sedition.** Investigations regarding alleged or suspected sedition may be based on either the Federal Sedition Statute or the UCMJ. Leads or allegations which prompt a sedition investigation by control offices may come from many sources. However, they are most often

based on information submitted by confidential sources which are contained in reports from other agencies or developed during the course of routine background investigations (BIs).

a. Investigations involving sedition may occur with equal frequency in either peacetime or periods of hostilities. Title 18, US Code, describes two types of sedition: seditious conspiracy and advocating the overthrow of the US Government.

(1) Seditious conspiracy. Title 18, US Code, Section 2384, makes it a specific crime to conspire to overthrow the US Government.

(a) Unlike the general conspiracy statute, which makes it a crime to conspire to commit any federal crime, the seditious conspiracy statute does not require the commission of an overt act towards fulfillment of the conspiracy's objective.

(b) The crime of seditious conspiracy is complete when two or more persons have entered into agreement to overthrow the government or to prevent, hinder, or delay the execution of any law of the US.

(c) Remember, seditious conspiracy is a conspiracy to actually overthrow and is distinct from a conspiracy to advocate overthrow.

(2) Advocating overthrow. Title 18, US Code, Section 2385, (also known as the Smith Act), enumerates specific types of activity which, if done with the intent to cause the overthrow of the government by force or violence, constitute sedition. The prohibited acts are—

(a) Advocating action and systematically teaching the duty or necessity of such overthrow.

(b) Using words to incite imminent lawless action with the specific intent of overthrowing the US Government.

b. Court decisions on the advocacy of overthrow have established that the advocacy must be calculated to incite persons to take action toward the violent overthrow of the government. The mere advocacy or teaching the forcible overthrow of the government as an abstract principle, divorced from any effort to instigate action, does not constitute the crime of sedition under the Smith Act.

c. The requirement for the advocacy (incite persons to take action) is of particular significance to CI agents. In any case alleging violation of the Smith Act, they will direct considerable effort toward proving that the oral or written material involved intended to incite listeners or readers to take action.

A-VIII-8. **Subversion.** Title 18, US Code, Section 2387 and 2388, and Article 94, UCMJ, make it criminal to advise or attempt to cause military members to mutiny. It makes it clearly illegal to try to undermine the loyalty, morale, or discipline of the military force of the US.

a. Many investigations of subversive activity are cases based on adverse loyalty information developed during routine—

(1) SSBI.

(2) SAEDA reports submitted by military or civilian personnel under AR 381-12.

(3) Reports from other intelligence and security agencies.

(4) Leads obtained directly from sources used in CI special operations.

b. Note that the terminology "criminal subversion," "subversive activity," "subversion," and "sedition against the military" are clues to the CI agent to turn to Title 18, US Code, Section 2387 and 2388, for detailed elements of the crime.

c. The objective of such an investigation may be to determine if there is a need for some type of administrative action; for example, removal of an individual from a sensitive assignment to protect the security of the military command.

A-VIII-9. **Responsibilities and Controls.**

a. The DCSINT, DA, exercises DA staff cognizance for CI investigations conducted by Army CI organizations. The DCSINT formulates policies for the conduct, management, direction, and control of CI investigations.

b. For the DCSINT, INSCOM maintains the ACCO for all Army CI investigations, special operations, and counterespionage projects. The ACCO exercises overall control and coordination of all Army CI investigations, and ultimate case control over all investigations.

c. The SCOs have been established in the theater support brigades of the 66th, 470th, and 500th MI Brigades, plus the 650th and 902d MI Groups. The SCOs have authority to initiate, direct, and terminate CI investigations in accordance with AR 381-20.

d. CI investigations must conform to laws and regulations. CI agents must report information accurately and completely. They maintain files and records to allow transfer of an investigation without loss of control or efficiency. Coordination with other CI or law enforcement organizations ensures that investigations are conducted as rapidly as possible. It also reduces duplication and assists in resolving conflicts when jurisdictional lines are unclear or overlap. CI investigations must be conducted as to avoid publicity. This is required to protect the rights of individuals and to preserve the security of investigative techniques.

A-VIII-10. **Investigative Plan.** When required, CI personnel formulate an investigative plan at each operational level down to and including the individual CI agent. The SCO dictates which element will write the investigative plan. Normally, that element will be the lead investigative element.

a. Although this list is not all encompassing, an investigative plan should include as many of the following planning considerations as applicable:

(1) Purpose of the investigation.

(2) Phases or elements of the investigation which have been assigned.

(3) Whether the investigation is to be conducted overtly or discreetly.

(4) Priority and time permitted for completion.

(5) Special instructions or restrictions.

(6) Information from the unit or office files.

(7) Definition of the problem.

(8) Methods and sources used, to include surveillance and polygraph support.

(9) Coordination required.

b. We must update the investigative plan as new developments arise, including an ongoing analysis of the results.

A-VIII-11. **Order of Investigation.** All investigations vary, and as such, all investigative plans will be different. The following actions are typically conducted during an investigation. Tailor investigative plans to each investigation. Investigative actions selected should be sequenced to ensure a swift and successful completion of the investigation.

a. Files and records checks for pertinent information.

b. Individual interviews for additional information and leads.

c. Exploitation of new leads and consolidation of all available data for analysis and planning a course of action (COA).

d. Surveillance, both physical and technical, of the SUBJECT.

e. Interrogation or interview of the SUBJECT to prove or disprove the allegations.

f. Polygraph examination.

A-VIII-12. **Investigative Techniques.**

a. The CI agent uses the following basic techniques in CI investigations and operations, as appropriate:

(1) Examine records to locate, gain access to, and extract pertinent data from diverse official and unofficial documents and records.

(2) Conduct interviews to obtain information. The type of interview conducted depends on the investigation.

(3) Use interrogation and elicitation techniques as additional methods to gather information.

(4) Conduct physical and technical surveillance to augment other investigative activities. See FM 34-5 (S) for a detailed explanation of surveillance operations, and AR 381-10, Procedures 5, 6, 8, and 9, for legal requirements pertaining to electronic surveillance, concealed monitoring, searches and examination of mail, and physical surveillance.

(5) Conduct search and seizure when necessary. Do not conduct searches unless directed by the SCO for the appropriate level commander. The CI agent may coordinate this activity with law enforcement agencies, depending on the nature of the investigation. The CI agent will consult with the supporting SJA to ensure that the requirements for establishing probable cause have been met. (Refer to AR 190-22, AR 195-5, and FM 19-20 for policy and techniques used in searches and seizures; and AR 381-10, Procedures 7 and 8 covering physical searches and search and examination of mail.)

A-VIII-13. **CI (SAEDA) Walk-in Interview.** A walk-in is defined as an individual who seeks out US Army Intelligence (USAI) to volunteer information which is believed to be of intelligence value.

a. When interviewing such persons, the CI agent must consider the Source's motives for divulging information. If the motive can be determined early in the interview, it can be valuable in evaluating the information supplied and in determining the nature and extent of the Source's knowledge and credibility. Motivation includes, but is not limited to—

(1) Ideology.

(2) Personal gain.

(3) Protection of self or family ties.

(4) Fear.

(5) Misunderstanding of the function and mission of USAI.

(6) Mental instability.

(7) Revenge.

(8) Compliance with AR 381-12.

(9) Awareness from attending SAEDA briefings.

b. The motivation may not always be known, and sources may not always be truthful about their motives. The primary concern of the CI agent is to obtain all information, both of intelligence and CI value. The CI agent should be alert to detect whether the Source provides leads for exploitation.

c. Walk-in sources who volunteer information, that USAI is not authorized by AR 381-10 to collect, will be referred to the proper local, state, military, or national authority. Information received from anonymous telephone callers or written messages will be handled the same way. If possible, fully identify all unsolicited sources of information.

(1) If the Source's information is of no interest to USAI, but may be of interest to another agency, refer the Source to the appropriate agency.

(2) If the Source refuses referral to the appropriate agency, the CI agent will fully debrief the Source concerning the information. The CI agent may furnish the information verbally to the appropriate agency; but in all cases, a written report will be provided to the agency concerned containing the details given by the Source.

(a) Provide information concerning the Source, except when the Source requests anonymity as a condition of providing information.

(b) Records of referrals and reports of information volunteered by unsolicited sources may be retained indefinitely if the information volunteered indicated the existence of a threat to life and property or the violation of law. If not, retention is authorized for no longer than 90 days, unless further retention is required by law or by Army regulation.

d. The following steps, in the order given, are basic to Walk-in Interviews:

(1) Put the Source at ease. After determining that a walk-in source has information of intelligence value, display the appropriate credentials.

(a) Take the Source to a private place to conduct the interview. The CI agent's initial attitude frequently affects the success of the interview. The atmosphere should be pleasant and courteous, but professional. In accordance with the Privacy Act of 1974, the Source must be given a four point Privacy Act Advisement to include authority, principle purpose, routine uses, and voluntary and mandatory disclosure, prior to the CI agent obtaining the Source's personal information. Ask the Source for some form of identification, preferably one with a picture.

(b) Record the pertinent data from the ID card and tactfully exit the room.

(c) Using the identity information just obtained from the Source, check the office source or informant files to see what, if any, information on the Source is on file. Determine if the Source is listed as a crank, has a criminal record, or has reported information in the past, and if so, what was the validity and value of that information.

(d) If the Source is listed as a crank or a nuisance continue with the interview, but include this information in the appropriate memorandum.

(2) Let the Source tell the story. Suggest that the Source start the story from the beginning, using the Source's own words.

(a) Once started, let the Source talk without interruption. The CI agent should, however, guide the Source back if the Source strays from the basic story. From time to time, interject a word of acknowledgment or encouragement.

(b) At no time, give any indication of suspicion or disbelief, regardless of how incredulous the story may seem.

(c) While the Source gives an account for the first time, take minimal notes. Taking notes could distract the Source or the CI agent. Instead, pay close attention and make mental notes of the salient points as a guide for subsequent detailed interviewing.

(3) Review the story with the Source and take notes. Once the Source has finished telling the basic story, he or she generally will freely answer specific questions on the details. Being assured that the information will be kept in strict confidence, the Source will be less apprehensive of your note taking.

(a) Start at the beginning and proceed in a chronological order, using the salient features of the Source's account.

(b) Interview the Source concerning each detail in the account so that accurate, pertinent information is obtained, meticulously recorded, and that the basic interrogatives are answered for every situation. This step is crucial.

(4) Develop secondary information. The story and background frequently indicate that the Source may have further information of significant intelligence interest. Also develop this information fully.

(5) Terminate the interview. When you are certain that the Source has no further information, close the interview in a manner which leaves a favorable impression.

(a) At this point in the interview, ask the Source, point blank, what motivated him or her to come in and report the information; even if the Source volunteered a reason earlier in the interview.

(b) Obtain a sworn statement from the Source, regarding the information, if appropriate. It is best to have the Source write (or type) the statement.

(c) Advise the Source of the Privacy Act of 1974 and ask the Source for full name; rank (for military or DOD civilian personnel) or occupation for non-DOD personnel; duty position, unit of assignment (for military or DOD civilian personnel); SSN, DPOB (required for military or DOD civilian personnel, requested for non-DOD personnel); type of security clearance and level of access; date of last SAEDA briefing; and full current address.

(d) Determine who else knows about the incident or situation, either directly or indirectly.

(e) Advise US sources of the provisions of the Privacy Act of 1974, and determine the Source's desires regarding the release of the Source's identity.

(f) Determine the Source's willingness to be recontacted by a member of USAI or another agency should the need arise regarding the information provided. Obtain recontact information from the Source (work or residence).

(g) Have the Source execute a Disclosure Warning and attach the affirmation to the report as an exhibit.

(h) Express appreciation for the information received.

e. In preparing for and conducting a Walk-in Interview, the CI agent—

(1) Should adapt to the intellectual level of the source, exercise discretion, and avoid controversial discussions.

(2) Must obtain all names and whereabouts of other individuals who may directly or indirectly know the same information.

(3) Must remember security regulations and make no commitments which cannot be fulfilled.

A-VIII-14. **CI (SAEDA) Source Interview.** A Source is a person who has direct personal knowledge concerning a factor series of facts. The important part of this statement is direct, personal knowledge of a fact. The CI agent is concerned with the person who gained this knowledge of an action or incident through one of the five senses. The walk-in volunteers information. The CI agent has to locate and convince a Source to talk and provide the desired information. The CI agent often must persuade a Source to answer questions.

a. The Source is important because this person can provide both direct evidence as well as data and leads. These may not be admissible in a legal proceeding, but may serve to aid further investigation.

b. The general principles observed in interviewing walk-ins also apply to Sources, but a few additional factors have a bearing on the questioning technique:

(1) The Source's reputation, social standing, profession, and the fact that the person's statements are recorded for possible use in court cause understandable psychological reactions. These psychological effects are occasionally discovered in the form of resistance to questioning or refusal to testify.

(2) Sources may not be able to keep personal prejudice from distorting the facts. Less conscientious persons may not even attempt objectivity.

(3) Individuals may not know they are capable of unwittingly distorting facts or that forgotten details are being replaced with products of their imaginations. The longer the time lapse between incident and interview, the greater the possibilities of imagination altering facts.

c. There are certain circumstances and conditions which may be present and which may affect the evaluation of information received from a Source.

(1) Physical condition: The Source's physical condition at both the time of the incident and at the time of the interview must be taken into account. Knowledge comes to an individual through one or more of a person's senses. If there are any limiting factors to an individual's sensory ability, questions may arise concerning the individual's competence in observation.

(2) Mental condition: Of similar importance is the Source's mental competency. A Source must be able to perceive, comprehend, and report what has happened to be considered competent. If one of these factors is missing or diminished, the individual will not be a good Source.

(3) Age:

(a) Once a child has reached the "age of reason," the child's testimony may have the same weight as that of an adult. This age is when a child is able to differentiate between fantasy and fact, and report factually what has happened. There are individual differences in this development process; but normally, the age of reason is considered to be seven or eight years. The likelihood of children bearing false testimony in deliberate attempts to influence situations is relatively slight. On the other hand, the demand of logic does not hamper their vivid imaginations; they do exaggerate.

(b) On the other end of the spectrum, senility or mental competence may be a factor.

(c) In either case, it is not wise to make generalizations about age when evaluating sources. However, it is important to be aware of the age factor and take that into consideration with each individual involved in a case.

(4) Objectivity: Probably one of the most important factors to be considered during the Source interview is objectivity.

(a) Normally, people observe and remember only those things of interest to themselves. Strong personal prejudices influence the way people see and remember things.

(b) When dealing with a Source, the CI agent must listen carefully to what is said to determine what these interests and prejudices are and what errors they may cause in the Source's responses, whether intentional or unintentional.

(c) Most errors of this type are unintentional and due to faulty memory. Careful questioning can discover this.

(5) Time: The average person's testimony will be distorted in one way or another. The brain will attempt to fill in any gaps by drawing on previous experiences. The more time that elapses between the incident and the questioning, the more the Source's story may become distorted. Unfortunately, the CI agent may not have control over the time factor; but in any case, attempt to interview the Source as soon as possible. This will enhance the validity of the Source's statement.

d. The CI agent's task is further complicated because the agent may deal with sources whose attitudes require the CI agent to change technique. The following are types of cases which require special treatment:

(1) Some sources may flatly refuse to talk because of possible danger to themselves. The CI agent should attempt to elicit cooperation by appealing to the Source's sense of patriotism or civic responsibility, pointing out it is in the individual's personal interest to talk, or leading the person into a logical path of reasoning. Discussing the Privacy Act of 1974 early may ease the Source's fears.

(2) Some sources are eager to demonstrate their knowledge to prove to themselves they are indispensable members of society. They may be braggarts, they may talk too much, or they may be a "know it all." The CI agent must be patient and critically weigh everything said, separating truth from fiction by asking pertinent questions and analyzing information carefully by comparing it with other known facts.

(3) Some sources are timid while others suffer from emotional stress and nervous tension. There may be occasions when much will be gained by asking the Source questions when he or she is extremely vocal due to an emotional condition. After the Source calms down, the CI agent should ask the questions again.

(4) A habitual liar is obviously a poor source, but there are occasions when such a person is the only source of direct evidence against a SUBJECT. In such an instance, do not ignore this person because of this weakness. Habitual liars usually contradict themselves; and if one can be made to repeat the story often enough, the truth may emerge.

(5) If possible, question a drunken source on the spot. At the risk of being led through a conversational maze, the CI agent should talk with the Source and strive to extract disclosures which the Source might not make if sober. You may use these statements later as a basis for a formal interview or interrogation of the Source.

e. Ideally, the CI agent should question all sources at the scene of the incident and obtain their first-hand knowledge while events are still vividly impressed on their minds. If this is the case, the CI agent should make arrangements to reinterview sources in a more formal manner later. If the CI agent arrives at the scene of an incident long after it has occurred, there will be time lags, so the CI agent should obtain the names of all sources from officials on the scene. The CI agent should take the following actions:

(1) Whenever possible, the CI agent should attempt to find out as much as possible about the Source and how he or she is related to the incident before the interview. Do this through

routine records checks. The CI agent is trying to determine if there are any obvious factors which would preclude this individual from being able to serve as a source. Gathering this type of information continues during the interview. Before starting the actual interview, the CI agent should review ail known details of the case and prepare questions for the Source. These questions should include those which help establish the Source's capability.

(2) As with other types of interviews, there are certain things which must be established before the main part of the interview. The proper approach will help establish the necessary rapport with the Source. The CI agent—

(a) Presents credentials and verbally verifies the name and rank of the individual. In many cases, you may ask for positive ID, such as a military ID card. The use of positive ID will be left to your discretion. However, do not allow the request for ID to interfere with the establishment of rapport with the Source.

(b) Quickly verifies that the person was indeed at the location at the time of the incident. If not, ascertain if this person knows of anyone who was there. It would probably be appropriate to ask why someone would believe that this person was there. You need to advise the individual that it is not his activities that are under investigation, but that you are trying to obtain information regarding what he might have seen or heard. Do not become antagonistic; other sources may have been mistaken. Maintain rapport. The CI agent may need to talk to this individual at another time. If the person admits to being at the scene, proceed with the interview.

(c) Ensures that the Source understands that the US Government considers your presence and all matters discussed during the interview to be official in nature and not to be discussed with anyone.

(3) Allow the Source to tell the story. As with the Walk-in Interview, allow the Source to tell the story in narrative format all the way through.

(a) Keep note taking to a minimum. Focus attention on the Source and listen to the story.

(b) Some sources may be reluctant to talk and tell their story. Some people may wish not to become involved; others fear having to go to court or other legal proceedings and face cross-examination; and some may fear reprisals. These people may need reassurance before they will talk freely. The CI agent—

1 Should spend the time necessary with these people to establish rapport; and attempt to determine why they are reluctant to talk.

2 May promise a Source confidentiality as a condition of providing information. Remember, this is the only promise that can be made. Ensure that the Source understands exactly what this means.

3 Must NOT make any other promises to these people. In most cases, a simple appeal to duty or patriotism may motivate a reluctant Source after rapport has been established.

(c) Again, once the Source is willing to talk, let the person tell the story all the way through.

(4) Ask clear, direct questions which elicit narrative responses. As with the Walk-in Interview, go back over the Source's story. The CI agent—

(a) Must develop the complete story from this Source.

(b) Must not assume what this Source means, based on previous interviews. Cover all information and incidents brought to your attention by the walk-in and any previous sources to ensure that this Source's observations are obtained.

(c) Develops any new information this Source identifies.

(d) Uses basic questioning techniques. The six basic interrogatives should form the basis for all questions. Ensure that the Source's responses are fully understood.

(e) Fully identifies leads mentioned by the Source, during the course of the interview. The CI agent must not assume any previous knowledge of any information provided by the Source.

(5) When terminating an interview, the CI agent—

(a) Obtains full identifying data on the Source, after developing the Source's story. Full identifying data includes: name (last name , first name, and middle initial); rank, branch (if applicable), SSN, DPOB, MOS or duty position, unit of assignment, residence address, expiration of term of service, anticipated TDY or permanent change of station (PCS) dates, security clearance, and access to classified information, including any special accesses.

(b) Ensures the Source prepares a handwritten statement before leaving the interview, if appropriate.

(c) Provides the Source with the appropriate Privacy Act Advisement. This is essentially the same as for other sources.

(d) Determines if the Source has discussed the incident with others, if so, obtain their identities.

(e) Determines if the Source is willing to be recontacted by USAI, if necessary. Obtain the Source's desires regarding recontact.

(f) Ensures the Source executes a Disclosure Warning. This will depend on the approach used in the interview.

(g) Leaves the Source with a good frame of mind and thanks the individual for cooperating.

f. Throughout the entire interview, from the first approach to termination, the CI agent must never express opinions concerning the case. Simply get the Source's story. Some individuals, upon hearing the CI agent's opinion, may change their story to what they think the CI agent wants to hear as opposed to what actually happened. Be precise in recording the information. The CI agent must accurately record what the Source said. Significant contradictions between this Source's story and those of other sources may be addressed in the "Agent's Notes" paragraph of the related memorandum.

g. Agent's notes from counterespionage interviews must be maintained. The notes whether handwritten, audio, or video taped, are part of the case file, and can be subpoened. Notes are important if a case goes to trial. The judge could dismiss the case or tell the jury to disregard the agent's testimony if the agent can not support testimony with notes made at the time of interview.

A-VIII-15. **CI (SAEDA) SUBJECT Interview**

a. When tasked by the SCO or ACCO, CI agents conduct an interview of the SUBJECT of an investigation.

b. The CI agent must advise the individual of rights under the provisions of the Fifth Amendment to the US Constitution or Article 31, UCMJ, as appropriate if the SUBJECT is suspected of criminal wrongdoing. The CI agent must also remember that the SUBJECT has the right to legal advice at any time before, during, or after the interview.

c. The CI agent should contact the SUBJECT and inform the individual of the reason for the interview, such as involvement in a security matter. The CI agent should tell the SUBJECT that the interview gives the individual an opportunity to refute, mitigate, or explain questionable or misleading information and to provide information not otherwise obtainable.

(1) If the SUBJECT is willing to be interviewed, the CI agent should arrange the time, date, and place for the interview.

(2) If the SUBJECT refuses to be interviewed or to answer questions, make an official record of the refusal.

d. Before the interview, the CI agent must gather all available information and pertinent leads. The CI agent—

(1) Carefully reviews preplanned questions for each interview so that only information specifically authorized by the control office is released to the SUBJECT during the interview.

(2) Conducts the interview in an area that is under the CI agent's control.

e. During conduct of SUBJECT Interview, the SUBJECT perceives the CI agent as a representative of the US Army. As such, the SUBJECT will regard the CI agent's every statement, question, or contact as part of the official proceeding, whether so intended or not. The CI agent—

(1) Will **NOT** make any off-the-record or unofficial remarks in the interview.

(2) Will **NOT** make any promises or commitments to the SUBJECT which are beyond the CI agent's legal authority to fulfill.

(3) Avoids statements or representations which may be construed as opinion or advice to the SUBJECT about past, present, or future actions. Does not argue with the SUBJECT or express personal viewpoints on any matter.

(4) Asks for a reason if the SUBJECT refuses to be interviewed, and records the SUBJECT's response. Does not exert any pressure in an attempt to change the SUBJECT's mind.

(5) Stops the questioning if the SUBJECT requests a lawyer. If the SUBJECT is subject to the UCMJ, assists the SUBJECT in contacting the Trial Defense Service, through the SJA, if necessary.

(6) Takes the following actions in the sequence listed, when conducting the interview.

(a) Dictate identifying data into a tape recorder before the SUBJECT arrives. Turn off the machine. However, recording interviews is neither required nor desired.

(b) Initially identify the SUBJECT; identify yourself and present credentials. Positively identify the SUBJECT through the use of a pictured ID card, recording all pertinent information from the ID card.

(c) Explain the general purpose and confidential nature of the interview.

(d) Obtain permission to record the interview. Explain that it will facilitate the preparation of a written transcript of the interview, which the SUBJECT will have an opportunity to review, correct, and sign under oath.

(e) Turn on the tape recorder.

1 The CI agent should take notes during the interview, even if it is being electronically recorded.

2 If the SUBJECT objects to the tape recorder, turn it off. Continue the interview taking notes as accurately as possible, while maintaining close attention to the SUBJECT's verbal answers and physical reactions.

3 A tape recording is an administrative convenience, but not having one will not hamper taking the sworn statement and preparation of the Investigative Memorandum for Record (IMFR).

(f) Administer a full explanation of rights (if required). Request the SUBJECT read and sign DA Form 3881 to acknowledge receipt of the explanation of rights and to record the individual's decision to exercise or waive the right to remain silent and to consult counsel. If the SUBJECT does not waive his or her rights, terminate the interview.

(g) In accordance with the Privacy Act of 1974, whenever CI agents interview a SUBJECT, they must give the SUBJECT a four-point Privacy Act Advisement.

1 The CI agent should provide the SUBJECT with two copies of the advisement statement. One copy is for the individual's retention, if desired; the other copy is for reporting purposes.

2 Before highlighting the four points, the CI agent should allow sufficient time for the SUBJECT to read the advisement statement.

3 The CI agent should then explain the points covered in the form by stating:

> The US Army is authorized to conduct CI investigations in accordance with government directives; the result of the inquiry will enable DA officials to determine the nature and extent of action necessary to ensure the security of the Army; the information obtained from the individual will be furnished to authorized government officials; and the disclosure of personal information to the US Army is voluntary. However, failure to disclose necessary and relevant information which impedes the investigation may have an adverse impact on obtaining or keeping a security clearance or employment with the DA.

(h) Explain to the SUBJECT the DA policy of allowing SUBJECTS of investigations every reasonable opportunity to explain, refute, or mitigate information which is developed during an investigation. Furthermore, that this is the SUBJECT's opportunity to provide whatever information the SUBJECT feels is appropriate.

(i) Ask if the SUBJECT is willing to take an oath.

1 If the SUBJECT is not, ask why not, and continue the interview.

2 If the SUBJECT is willing to take an oath of truthfulness, an appropriate oath is: "Do you affirm that the statements you are about to make are the truth, the whole truth, and nothing but the truth?" Additional remarks such as "So help you God" are unnecessary and may be offensive.

(j) Ask the SUBJECT to state his or her name, rank, SSN, DPOB, unit of assignment, duty position, and residence address for the record.

(k) Conduct the interview using prepared questions designed to elicit narrative answers. These prepared questions are only a guide and are not intended to be the only questions asked. The CI agent must fully develop all information provided by the SUBJECT. Accurately record and report all answers.

(l) Only if tasked by the ACCO or SCO, determine the SUBJECT's willingness to submit to a polygraph examination. If a tape recorder is used, turn it off before asking this question.

(m) Obtain a sworn statement, preferably in the SUBJECT's own handwriting, before ending the interview. If illegible, prepare a typewritten sworn statement for the SUBJECT to review and sign. Include the original, handwritten statement as an attachment to the IMFR. Never destroy the original statement.

(n) Consistent with the offense the SUBJECT is under investigation for and the evidence available, arrangements for detention should be made prior to SUBJECT Interview.

(o) Remind the SUBJECT of the confidential and official nature of the interview and not to discuss it with anyone.

(p) Thank the SUBJECT for his or her cooperation and terminate the interview.