# COUNTERINTELLIGENCE OPERATIONS

## CHAPTER 1. INTRODUCTION

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1—1-5</td>
<td></td>
</tr>
</tbody>
</table>

## 2. ORGANIZATION AND EMPLOYMENT

### Section I. General

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-1—2-3</td>
<td></td>
</tr>
</tbody>
</table>

### Section II. CONUS and theaters of operation

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-4—2-7</td>
<td></td>
</tr>
</tbody>
</table>

### Section III. Military intelligence group (Counterintelligence) ASCOM

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-8—2-13</td>
<td></td>
</tr>
</tbody>
</table>

## CHAPTER 3. INVESTIGATIVE LEGAL PRINCIPLES

### Section I. General

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-1—3-4</td>
<td></td>
</tr>
</tbody>
</table>

### Section II. Obtaining evidence

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-5—3-11</td>
<td></td>
</tr>
</tbody>
</table>

### Section III. The sworn statement

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-12—3-28</td>
<td></td>
</tr>
</tbody>
</table>

## CHAPTER 4. BASIC INVESTIGATIVE TECHNIQUES AND PROCEDURES

### Section I. Introduction

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-1—4-3</td>
<td></td>
</tr>
</tbody>
</table>

### Section II. Records examination

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-4—4-6</td>
<td></td>
</tr>
</tbody>
</table>

### Section III. Interviews

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-7—4-15</td>
<td></td>
</tr>
</tbody>
</table>

### Section IV. Interrogations

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-16—4-18</td>
<td></td>
</tr>
</tbody>
</table>

### Section V. Elicitation

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-19—4-22</td>
<td></td>
</tr>
</tbody>
</table>

### Section VI. Surveillance

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-23—4-30</td>
<td></td>
</tr>
</tbody>
</table>

### Section VII. Collection and handling of physical evidence

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-31—4-35</td>
<td></td>
</tr>
</tbody>
</table>

### Section VIII. The special agent as a witness

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-36—4-38</td>
<td></td>
</tr>
</tbody>
</table>

### Section IX. Special situations

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-39—4-40</td>
<td></td>
</tr>
</tbody>
</table>

## CHAPTER 5. TECHNICAL INVESTIGATIVE SERVICES

### Section I. General

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5-1—5-2</td>
<td></td>
</tr>
</tbody>
</table>

### Section II. Audio surveillance

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5-3—5-5</td>
<td></td>
</tr>
</tbody>
</table>

### Section III. Surreptitious entry and Investigative photography

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5-6—5-9</td>
<td></td>
</tr>
</tbody>
</table>

### Section IV. False documentation and secret writing

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5-10—5-11</td>
<td></td>
</tr>
</tbody>
</table>

### Section V. The polygraph

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5-12—5-20</td>
<td></td>
</tr>
</tbody>
</table>

## CHAPTER 6. SOURCES OF INFORMATION

### Section I. General

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6-1—6-2</td>
<td></td>
</tr>
</tbody>
</table>

### Section II. Human sources

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6-3—6-5</td>
<td></td>
</tr>
</tbody>
</table>

### Section III. Documentary sources

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6-6—6-9</td>
<td></td>
</tr>
</tbody>
</table>

### Section IV. Technical/materiel sources

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6-10—6-11</td>
<td></td>
</tr>
</tbody>
</table>

### Section V. Liaison

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6-12—6-15</td>
<td></td>
</tr>
</tbody>
</table>

## CHAPTER 7. INVESTIGATIVE REPORTS

### Section I. Introduction

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7-1—7-4</td>
<td></td>
</tr>
</tbody>
</table>

### Section II. Purpose and use of counterintelligence investigative reports

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7-5—7-11</td>
<td></td>
</tr>
</tbody>
</table>

## CHAPTER 8. PERSONNEL SECURITY INVESTIGATIONS

### Section I. General

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8-1—8-2</td>
<td></td>
</tr>
</tbody>
</table>

### Section II. Conduct of background investigations

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8-3—8-19</td>
<td></td>
</tr>
</tbody>
</table>

## CHAPTER 9. COMPLAINT TYPE INVESTIGATIONS

### Section I. General

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9-1—9-4</td>
<td></td>
</tr>
</tbody>
</table>

### Section II. Sabotage investigations

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9-5—9-7</td>
<td></td>
</tr>
</tbody>
</table>

### Section III. Espionage investigations

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9-8—9-12</td>
<td></td>
</tr>
</tbody>
</table>

### Section IV. Treason investigations

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9-13—9-16</td>
<td></td>
</tr>
</tbody>
</table>

---

*This manual supersedes FM 30–17, 28 February 1968.*

The Pentagon Library
Rm 1A518, Pentagon
Washington, D.C. 20310
SECTION V. Sedition investigations ........................................ 9-17—9-21 9-6
VI. Subversive activity and disaffection investigations ................ 9-22—9-24 9-7

CHAPTER 10. COUNTERINTELLIGENCE SURVEYS
AND INSPECTIONS

Section I. Counterintelligence surveys ..................................... 10-1—10-2 10-1
II. Preparation for counterintelligence surveys .......................... 10-3—10-5 10-2
III. Conduct of counterintelligence surveys .............................. 10-6—10-13 10-3
IV. Counterintelligence inspections ....................................... 10-14—10-16 10-7
V. Reports of counterintelligence surveys and inspections .......... 10-17—10-18 10-9
VI. Security education ......................................................... 10-19—10-22 10-9

CHAPTER 11. COUNTERINTELLIGENCE TECHNICAL
SURVEYS AND INSPECTIONS

Section I. General ............................................................ 11-1—11-2 11-1
II. Conduct of counterintelligence technical surveys and inspections .... 11-3—11-8 11-2

CHAPTER 12. CONVENTIONAL COMBAT OPERATIONS

Section I. Introduction ....................................................... 12-1—12-2 12-1
II. Functions ........................................................................ 12-3—12-6 12-1
III. Planning and conduct of operations .................................. 12-17—12-14 12-4
IV. Tactical support operations ............................................. 12-15—12-16 12-12

CHAPTER 13. STABILITY OPERATIONS

Section I. Introduction ....................................................... 13-1—13-2 13-1
II. Counterintelligence operations .......................................... 13-3—13-7 13-2
III. Operational techniques and procedures ............................. 13-8—13-14 13-5

CHAPTER 14. INTERRELATIONSHIPS

Section I. Introduction ....................................................... 14-1 14-1
II. Relationship with civil affairs ......................................... 14-2—14-9 14-1
III. Relationship with military police .................................... 14-10—14-12 14-3
IV. Relationship with psychological operations ......................... 14-13—14-14 14-4
V. Relationship to other intelligence elements .......................... 14-15 14-4

APPENDIX A. REFERENCES .................................................. A-1

B. INVESTIGATIVE REPORTS ................................................ B-1
C. COUNTERINTELLIGENCE SERVICES REPORTS ..................... C-1
D. COUNTERINTELLIGENCE SURVEY CHECKLIST ..................... D-1
E. NARCOTIC AND DRUG ABUSE GUIDE ................................ E-1

INDEX ............................................................................... Index-1
CHAPTER 1
INTRODUCTION

1–1. Purpose and Scope

a. This manual provides operational guidance for Army counterintelligence personnel and outlines standard investigative procedures for employment by counterintelligence elements and units of the United States Army.

b. This manual includes a general orientation on several types of counterintelligence elements existing within the Army and describes in greater detail the basic techniques and procedures employed by Army counterintelligence personnel in both peace and wartime situations. Specific applications of these techniques and procedures are covered in those chapters which deal with counterintelligence investigations and services.

c. Material in this manual is limited to those aspects of counterintelligence which are the specific responsibilities and functions of counterintelligence personnel and units in accordance with AR 381–103.

d. The material presented herein is applicable in both nuclear and nonnuclear warfare and in chemical, biological, radiological and internal defense environments as well as to peacetime counterintelligence operations.

e. Users of this manual are encouraged to submit recommended changes or comments to improve the manual. Comments should be keyed to the specific page, paragraph, and line of the text in which the change is recommended. Reasons should be provided for each comment to insure understanding and complete evaluation. Comments should be prepared using DA Form 2028 (Recommended Changes to Publications) and forwarded direct to the Commanding Officer, US Army Combat Developments Command Intelligence Agency, Fort Huachuca, Arizona 85613.

1–2. Counterintelligence Personnel

As used in this manual, the terms “counterintelligence personnel” and “Special Agents” are synonymous and include officers with MOS Code 9666—Counterintelligence Officer, warrant officers with MOS Code 971A—Counterintelligence Technician, enlisted men with MOS Code 97B—Counterintelligence Agent and DA civilians who have been accredited as Special Agents by the Chief of Personnel Operations, Department of the Army, and who are assigned to duty for the performance of counterintelligence functions. Accreditation includes issuance of identifying badge and credentials in accordance with AR 640–20.

1–3. Scope of Counterintelligence Activities

The mission of counterintelligence elements and units is to support the commander through the detection of treason, espionage, sabotage, sedition, subversive activity, and disaffection, and the prevention and neutralization of espionage and sabotage for the protection of the US Army. In the fulfillment of this mission, counterintelligence personnel and units engage in a broad range of operational activities, with direction and guidance from higher authority, within the areas of its jurisdiction to include those activities responsible for—safeguarding defense information; protecting Army functions and property such as facilities which have classified defense contracts or that have been designated as key defense installations; conducting personnel security investigations for Army personnel and contractor employees under the Defense Industrial Security Program; conducting counterintelligence surveys, services, and inspections; and conducting investigative activities authorized in connection with civil disturbances within the United States, the District of Columbia, the Commonwealth of Puerto Rico, and the United States territories and possessions. Counterintelligence operations may be divided into the following three categories:

a. Counterintelligence Investigations. This operational category constitutes the bulk of the counterintelligence workload worldwide, and in-
cludes specific investigations of individuals and incidents which, for the most part, are conducted in an overt but discreet manner. Personnel security investigations (PSI) and complaint-type investigations (CTI) are included in this category.

b. Counterintelligence Services. This operational category encompasses specific security services provided by counterintelligence personnel and units to assist commanders at all echelons in planning, implementing, and maintaining proper and adequate safeguards against the threats of sabotage, espionage, and subversive activity. These services include counterintelligence surveys and inspections, security education and training programs, and technical surveys and inspections.

c. Counterintelligence Special Operations. Special operations which are concerned mainly with sophisticated and highly specialized techniques in the areas of counterespionage, countersabotage, and countersubversion are discussed in the classified supplement to this manual, FM 30–17A.

1–4. Limitations of Counterintelligence Operations

The jurisdiction and scope of authorized investigative techniques in counterintelligence operations will vary according to legal considerations, operational circumstances, and areas of operations. The following types of limiting directives may restrict the jurisdiction of counterintelligence elements and preclude or inhibit employment of certain investigative techniques and procedures described in this manual:

a. Delimitations Agreement. AR 381–115 prescribes the Army's counterintelligence investigative jurisdiction and its coordinating responsibilities with respect to the Federal Bureau of Investigation (FBI), Department of Justice; the Naval Investigative Service (NIS), Department of the Navy; and the Office of Special Investigations (OSI), Department of the Air Force.

b. National Security Directives. Operational limitations and coordinating responsibilities for United States agencies conducting security investigations or intelligence operations in foreign areas are set forth in classified policy directives issued by the National Security Council. These directives are normally implemented within the Army by operational instructions prepared and disseminated by the Office of the Assistant Chief of Staff for Intelligence, Department of the Army.

c. Status of Forces Agreements. Agreements between the United States and foreign nations in which US Army units are stationed normally include clauses delimiting the jurisdiction and scope of activities of counterintelligence agencies. Implementing directives within the Army are normally promulgated by the major command directly concerned with the “status of forces agreement.”

d. DOD Directive 5200.27. This directive is a restatement of the limits applied to military counterintelligence activities to include those persons or organizations affiliated with the DOD. A person, group of persons, or organization is considered to be affiliated with DOD if the individuals involved are:

(1) Employed by or contracting with DOD or any activity under the jurisdiction of DOD, whether on a full time, part time, or consultative basis;

(2) Members of the Armed Forces on active duty or National Guard members in a reserve or retired status;

(3) Residing on, having authorized access to, or conducting or operating any business or other function at any DOD installation or facility;

(4) Authorized access to defense information;

(5) Participating in other authorized DOD programs to include persons upon whom investigations have been initiated under the following:
   (a) AR 230–2—Personnel Policies and Procedures.
   (b) AR 604–20—Security Requirements for Personnel in Information and Education Activities.
   (c) AR 690–1—Civilian Applicant and Employee Security Program.
   (d) AR 930–5—American Red Cross Service Program and Army Utilization.
   (e) DOD Regulation 5220.22R—Industrial Security Regulation.

(6) Applying for or being considered for any status described above to include applicants for military service, preinductees, and prospective contractors.

1–5. Basic Principles of Counterintelligence Operations

Regardless of the type of operation, or of operational circumstances, all counterintelligence operations adhere to certain basic principles:
a. **Conformance to Mission.** The basic mission requires that every counterintelligence operation support the commander, contribute to the security of the US Army, and be within the scope of activities prescribed in the mission of counterintelligence units and personnel of the US Army.

b. **Avoidance of Publicity.** The “golden word of intelligence is silence.” This is an established principle in all intelligence operations, and one that is especially applicable to counterintelligence activities. There will be occasions when it is desirable to publicize successfully completed investigations of espionage or other activities to deter others from engaging in such activities, or to encourage voluntary reporting of information (i.e., publicizing the location where information of counterintelligence interest may be reported). In this, however, counterintelligence personnel must exercise discretion and avoid individual publicity.

c. **Objectivity.** Counterintelligence elements are primarily factfinding agencies whose purpose is to collect and report factual data upon which responsible commanders may base decisions relative to the security of their commands. It is absolutely essential that counterintelligence operations be planned, executed, and reported in a completely objective manner. The principle of objectivity is perhaps most important in the reporting phase of operations. All information pertinent to the issue, whether favorable or unfavorable to an individual or organization, whether consistent with or contrary to previously reported information, must be recorded and reported accurately and objectively. However, important derivative information, indicators and/or leads must not be overlooked or ignored because they are not based on factual information at the time. Such leads may be confirmed or substantiated in the future, or may contribute significantly in other ways to the successful conclusion of the investigation.

d. **Confirmation.** Regardless of the probable reliability of the source of any item of counterintelligence information, independent confirmation will always be sought in all counterintelligence investigations. Confirmation may be achieved by the use of additional investigative techniques, by consulting additional sources of information, and by regularly testing the reliability of those sources which are utilized over an extended period of time. Confirmation of small details, which in themselves appear insignificant, is fundamental to all investigations and will often prove the only reliable means of establishing the true status of a person suspected of participation in hostile intelligence activities. However, reporting of information to permit initiation of preventative action, when an immediate threat to security appears probable, should not be delayed pending confirmation.

e. **Offense.** One of the most important principles of counterintelligence operations is a well-planned positive program of offensive actions to thwart actions of the opposition. The neutralization of hostile espionage and subversive organizations is especially dependent on positive, offensive actions for success. Offensive counterespionage details are discussed in FM 30-17A, the classified supplement to this manual.

f. **Flexibility.** Each counterintelligence element, from the individual to the largest operational unit, must be able to respond immediately and positively to changes in the situation, e.g., a sudden influx of large numbers of refugees or a rapid change from a peacetime to a hostile environment.

g. **Continuity.** Continuity of action in counterintelligence investigations is imperative particularly in connection with case control personnel. Continuity can be realized only through meticulous efforts to have detailed results of investigations properly recorded in official files. The full status of any investigation at any given time should be as clear to successors as to those who originally obtained or processed the information collected or received.

h. **Coordination.** In all counterintelligence investigations and operations, coordination consistent with security considerations and the policy of the command is maintained with units and agencies having a direct interest.
CHAPTER 2
ORGANIZATION AND EMPLOYMENT

Section I. GENERAL

2—1. Introduction
This chapter provides a general orientation on the organization and employment of counterintelligence elements. Continuing research and development studies and the evolutionary changes in the Army bring about changes in organizational structures. These changes affect tactical counterintelligence units more than others; therefore, reference to the 30-series TOE for detailed information on the current tactical counterintelligence organizations is recommended.

2—2. Organizational Principles and Considerations

a. Counterintelligence elements are organized in consonance with the principles of organization described in FM 100-5 and FM 101-5. Organization along functional lines with maximum internal flexibility is essential to insure responsiveness to changes in operational environments, shifts in emphasis or priorities, and variances in the nature and degree of the threat to the supported command.

b. Considerations which influence the organization of counterintelligence elements include:

(1) Mission, type, strength, location, geographic responsibility, and scope of activities of the supported command.

(2) Intelligence and counterintelligence estimates and studies setting forth the characteristics of the area of operation.

(3) Intelligence mission assigned to the supported command, together with specific intelligence directives and related delimiting policy directives.

(4) Counterintelligence mission prescribed by the supported command which indicates relative emphasis to be given to the various functions enumerated in AR 381-103 and AR 381-130.

(5) Availability of counterintelligence personnel, including the availability of qualified linguists in foreign areas.

(6) Threat posed by hostile intelligence.

2—3. Employment of Counterintelligence Personnel

a. Basic policies governing the employment and utilization of counterintelligence personnel are contained in AR 381-103. Personnel may be employed in units which consist almost exclusively of counterintelligence personnel (e.g., military intelligence (MI) groups in CONUS), or they may be assigned to intelligence units which contain other intelligence specialist elements (e.g., MI groups, battalions, or companies assigned to either tactical or nontactical units).

b. The specific needs of some nonintelligence units and installations, particularly those responsible for weapons or materiel of a classified nature, will sometimes require the assignment of counterintelligence personnel on a permanent basis. US Army missile commands are examples of units which include organic counterintelligence personnel within their TOE. Details regrading the employment of counterintelligence personnel in assignments of this type are outside the scope of this manual.

Section II. CONUS AND THEATERS OF OPERATION

2—4. The US Army Intelligence Command
The US Army Intelligence Command (USAINTC), Fort Holabird, Maryland, under the supervision of the Chief of Staff, Department of the Army, is responsible for the tasking and controlling of all Army CI activities in support of
the CONUS-based major commands, Puerto Rico and the US Virgin Islands on a geographic area basis. USAINTC exercises control office functions for personnel security investigations which originate in United States Army, Europe (USAREUR); United States Army, Pacific (USARPAC); United States Army, Alaska (USARAK); and United States Army, Southern Command (USARSO). It also performs other intelligence-counterintelligence functions as assigned by Department of the Army and makes recommendations to higher and collocated echelons on these matters. Military Intelligence Groups (CI) are assigned to USAINTC as operating elements with the mission of providing CI support to all designated US Army operations in specific geographic areas. An MI group is collocated with each of the headquarters of CONUS armies and the Military District of Washington. The area of responsibility of a MI group normally coincides with the geographic area of the Army to which it is assigned. Because of the Delimitations Agreement and the limited intelligence mission of the Army in CONUS, counterintelligence operations consist primarily of security investigations and services conducted throughout the geographic area of responsibility. Figure 2-1 illustrates the organization of the USAINTC with its subordinate MI groups. Figure 2-2 is a chart of the functional organization of a typical CONUS MI group. Subordinate elements of the group—regions, field offices and resident offices—are strategically located throughout each of the geographic areas of responsibility. The regional office or headquarters is the principal operational element of most CONUS groups and normally is responsible for a specific geographic area; this area may correspond to a single political subdivision such as a county, or be comprised of multiple political subdivisions such as a group of counties, or portions of one or more states.

2-5. Tactical Counterintelligence Elements
The concept of integration of all intelligence specialists at tactical levels is contained in FM 30-9. Assigned to the field army is a MI battalion or
group which has subordinate MI units attached to corps, divisions, and separate brigade-sized units to provide intelligence support. These units contain CI tactical support elements. Military intelligence units supporting corps, divisions, and separate brigades/ armored cavalry regiments will move with the supported units when restationed or deployed overseas. All tactical intelligence units are controlled by the commander of the unit to which they are attached, with general staff supervision exercised by the intelligence officer, S2/G2 or the Assistant Chief of Staff, Intelligence. The CI elements of these units are operationally restricted to the confines of the military reservation where they are stationed; however, in CONUS local jurisdictional agreements between these units and the CONUS MI groups facilitate accomplishment of the mission.

2-6. Special Counterintelligence Units

The Department of Defense, the US Continental Army Command and the US Army Intelligence Command have assigned counterintelligence personnel and units over which they exercise operational control. The operations of these units are accomplished within the area of jurisdiction of the five MI groups in CONUS and, at times, cross one or more jurisdictional boundaries. Special Agents of these units will normally notify the appropriate MI groups and/or the senior intelligence staff officer of the major command of their presence in the area and, when permissible, state their mission.

2-7. Theaters of Operation

The employment, functions, and operational concept of counterintelligence elements in a theater of operations are prescribed in FM 30-9. Counterintelligence units must maintain a close working relationship with other intelligence agencies, both civilian and military, with civil affairs and with military police elements at all echelons within the theater in accordance with existing theater policies. Counterintelligence operations may be divided into two levels of activity, theater army and field army.

a. Theater Army. Counterintelligence missions and activities do vary considerably between theaters of operation and between peacetime and pe-
rions of hostilities. Differences are based on the
number of installations and troop strengths
within a theater, the nature and magnitude of the
hostile threat in the area, and the relations and
agreements with host country and allied govern-
ments. Some situations may require deviations
from the general principles of organization and
control, although deviation is not the normal pro-
cedure. Fundamentally, theater army is a plan-
ning and coordination headquarters that retains
for itself only those functions which cannot be
accomplished efficiently by lower echelons. The-
ater army may delegate the responsibility for
rear areas to Theater Army Support Command
(TASCOM). The mission of rear area security in-
cludes all aspects of counterintelligence. To ac-
complish the counterintelligence portion of rear
area security, a MI Group (CI), (sec III), cons-
isting predominantly of counterintelligence per-
sonnel, will be assigned to TASCOM or other re-
 sponsible command. To provide area coverage,
subordinate companies, detachments, or regions
will be located strategically throughout the area.
Included in this MI Group (CI) is a central rec-
ords facility which will serve all security and in-
telligence elements of both theater army, and
field army, as well as elements of other US mili-
tary services.

b. Field Army. The field army is provided coun-
terintelligence support by a CI company organic
to the field army MI battalion and by CI elements
organic to the military intelligence units attached
to corps, divisions and separate brigade-sized or-
ganizations. However, military intelligence units
attached to corps and divisions are controlled by
the corps and division commanders, respectively,
with general staff supervision exercised by the
respective G2. The field army has a rear area se-
curity mission, including all aspects of counterin-
telligence, similar to theater army. The CI com-
pany assigned to the MI Battalion (Field Army)
normally will have the counterintelligence mis-
sion from division rear to the field army rear
boundaries. The unit may have several stations
strategically located to facilitate control and com-
munication with a number of small mobile teams
working out of each station.

Section III. MILITARY INTELLIGENCE GROUP
(COUNTERINTELLIGENCE), ASCOM

2–8. General

a. Mission and Functions. A Military Intellig-
ence Group (Counterintelligence) is assigned to
the area support command (ASCOM). It provides
counterintelligence specialist support to theater
army support command (TASCOM) for the se-
curity of US personnel and installations within
the TASCOM area. The group accomplishes its
mission by—

(1) Supporting TASCOM, ASCOM, and its
subordinate area support groups (ASGP) by
providing specialized assistance in the field of
counterintelligence.

(2) Commanding, controlling, and supervis-
ing operational, administrative, and logistical
functions of subordinate elements.

(3) Planning CI operations and activities to
achieve maximum security for army units and in-
stallations within the TASCOM area and to
achieve maximum neutralization of hostile es-
pionage activities.

(4) Exercising centralized control and man-
gelement of special operations in the areas of coun-
terespionage, countersabotage, and countersub-
version within the TASCOM area.

(5) Supervising the operation of a central
records facility on personnel of intelligence interest for TASCOM and other elements within the
theater army.

(6) Providing liaison with parallel US, host
government, and allied nation intelligence and se-
curity activities.

(7) Exercising control of security investiga-
tions to include personnel security investigations
(PSI) and complaint-type investigations (CTI).

(8) Supervising and coordinating security
services to include CI surveys and inspections, se-
curity education and training programs, and
technical surveys and inspections.

(9) Providing CI support for army nuclear
weapon systems and facilities.

(10) Coordinating the allocation of counterin-
telligence personnel resources, based on ASCOM
priorities, functional requirements, and disposi-
tion of army units and hostile elements.

b. Organization. Figure 2–3 depicts the organi-
zation of the MI Group (CI), ASCOM.

2–9. Functions

a. The MI Group (CI), ASCOM, coordinates its
operations through direct liaison with the MI Battalion (Field Army); the MI group, theater army; and other services or joint intelligence and security elements at theater level. This group maintains liaison with intelligence and security services of host governments, allied nations, and the United States, as well as with military police and civil affairs (CA) units which may be primary sources of intelligence information. Host government agencies may be responsible for providing information on which to base clearance actions on indigenous labor force personnel requested by a TASCOM unit, depending on pertinent status of forces agreements, or other appropriate agreements.

b. The HQ, MI Group (CI), ASCOM, (fig 2-4) is organized and trained to operate against the hostile clandestine threat. It exercises centralized control and management of counterespionage, countersabotage, and countersubversive operations within TASCOM. Further, the group is responsible for unified planning and operations against hostile elements whose activities transcend ASGP boundaries. As a result of these operations, this group can collect intelligence information on guerrilla forces. The MI Group (CI), ASCOM, is not organized, equipped, or trained to conduct reconnaissance patrols or other combat missions against guerrilla forces.

c. The MI Group (CI), assists TASCOM unit commanders in the exercise of their security responsibilities and will conduct interviews, inquiries and other actions necessary to meet USAINTC requirements on PSI and CTI. This group will exercise control and management of such investigative activities conducted by its subordinate units. This group also exercises centralized control and management of personnel security actions. The MI group headquarters depends on the theater common-user signal system for communication with subordinate elements and on the personnel and administration (P&A) battalion, ASCOM, for the production of P&A reports and the maintenance of P&A records.

d. The MI Group (CI), has no imagery interpretation capability. When an air reconnaissance and surveillance unit is assigned to ASCOM, a cellular-type (TOE 30–600) MI detachment with appropriate imagery processing and interpretation capabilities can be assigned to the group.

2-10. Military Intelligence Detachment (Central Records Facility)
The MI Detachment (Central Records Facility),
Figure 2-4. HQ, MI Group (CI).

(Fig 2-5) maintains files on personnel of intelligence interest to theater army and provides direct support (DS) to theater army intelligence units. The detachment performs its mission by—

a. Receiving, screening, extracting, and filing reports from detachments of the MI Group (CI), and other intelligence units of the theater and field armies.

b. Opening new dossiers and updating existing dossiers with incoming reports.

c. Maintaining a central index and a dossier file.

d. Responding to queries from within the group and from other theater army intelligence units, conducting file searches and providing support to

Figure 2-5. MI Detachment (Central Records Facility).
counterespionage, countersabotage, and counterversive operations.

e. Maintaining operational files for the MI Group (CI).

2-11. Functions
The MI Detachment (Central Records Facility), normally is in the immediate vicinity of the MI Group headquarters and depends on the headquarters for its administrative communication and logistical support. The detachment operates under the direct supervision of the group S3. It maintains its own message center and teletype terminal and provides its own control of classified documents.

2-12. Military Intelligence Company (Counterintelligence)
The Military Intelligence Company (Counterintelligence), (fig 2-6) conducts operations that will enhance personnel and installation security of US personnel and facilities in the ASGP area of responsibility and reduce the hostile clandestine threat thereto. The company accomplishes its mission by—

a. Assisting in the screening of indigenous personnel for intelligence operational leads and for suspected dissidents.

b. Conducting CI surveys, inspections, and technical inspections.

c. Conducting counterespionage, countersabotage, and counterversive operations.

d. Processing requests for clearance of indigenous labor force personnel.

e. Assisting ASGP in security education programs.

f. Conducting interviews, record checks, and other investigative activities in response to requirements of PSI and CTI.

2-13. Functions
a. The MI Company (CI), is attached to ASGP for administrative support. It provides security support for ASGP and army units or facilities located within the ASGP area. Subordinate elements of the company are located within the ASGP area at locations that facilitate counterintelligence operations. The disposition of personnel resources is based on requirements of the MI Group (CI) and the ASGP.

b. The company is in the immediate vicinity of ASGP headquarters. The MI Company (CI) depends on ASGP for normal combat service support. It operates under the staff supervision of the Assistant Chief of Staff for Security, Plans, and Operations in developing the command's security program. The Assistant Chief of Staff for Security, Plans, and Operations levies requirements directly on the company. He also determines requirements for interrogation personnel or other MI specialist support and directs the utilization of such assets when they are provided. Unit requests for CI surveys, inspections, and technical inspections go to ASGP for approval and designation of priorities for accomplishment by the company. Resulting reports go directly to the requesting unit with information copies to ASGP.
CHAPTER 3

INVESTIGATIVE LEGAL PRINCIPLES

Section I. GENERAL

3-1. Introduction

a. Although only a small percentage of counterintelligence investigations will result in the prosecution of an offender before any type of court, investigations should be conducted with an awareness of the principles of law and the rules of evidence which govern the prosecution of any criminal activity. The majority of counterintelligence investigations, particularly personnel security investigations, usually require only administrative actions, in which the actual legal requirements regarding evidence are much less stringent than in the case of court proceedings. It is nevertheless essential that counterintelligence personnel have a basic understanding of the legal principles and procedures involved in conducting an investigation, for at least three reasons:

(1) To be able to apply them in cases where they are strictly applicable;
(2) To be guided by them in cases not foreseen, but where there is no time to seek specific guidance or assistance; and
(3) To be able to recognize those cases where specific guidance or assistance must be obtained prior to proceeding further.

b. The legal principles covered in this chapter are designed to aid counterintelligence personnel in recognizing basic legal problems that might arise during an investigation and to provide guidance when evidence is sought from an accused or suspect. Basic legal principles are applied in specific investigative situations; accordingly, counterintelligence personnel should obtain advice from a staff judge advocate or legal officer to be certain that full consideration is given to recent court decisions interpreting statutes and regulations.

3-2. Evidence

a. In the broadest sense, “evidence” consists of all matters which are logically relevant to the resolution of any issue of concern. Evidence may include the testimony of witnesses, documents, objects, photographs, and sound and video recordings as well as the results of scientific tests.

b. Normally, only evidence that has been lawfully obtained is admissible in courts. “Lawfully obtained” means obtained in accordance with the legal principles of the jurisdiction concerned. Evidence which is admissible in a court proceeding is always preferred in an administrative hearing as well, because of the greater weight logically accorded it by reasonable men. The normal job of the Special Agent is to conclude his investigation with all his evidence having been lawfully obtained and admissible in court, and therefore in any board.

3-3. Criminal Offenses

a. A “criminal offense” or “crime” is generally defined as a violation of penal law. In the United States, penal law is largely statutory in form. The statute prescribing a criminal offense will usually include in some detail the acts or omissions constituting the offense.

b. The responsibility of counterintelligence personnel for investigating criminal offenses is specified in paragraph 1-3 above. Chapter 9 further discusses these offenses.

3-4. Rules of Evidence

a. Every court or board has rules concerning the evidence that it will accept. The Manual for Courts-Martial, United States, 1969 (Rev. Ed.), contains the “rules of evidence” in cases before courts-martial. The “rules of evidence” for federal and state courts may be found in legal texts or other published volumes of law. “Rules of Evidence” for administrative boards, however, to whatever extent they exist, may or may not be contained in the regulation pursuant to which the board was established. Most often, AR 15-6 applies, and, as a result, the exclusionary rules of
Section II. OBTAINING EVIDENCE

3-5. Introduction

This section discusses the constitutional rights of a suspect or accused person during an investigation and the legal ramifications when obtaining evidence by means of interviews or interrogations, search and seizure, and apprehension. A violation of legal principles involved in these means will substantially, if not completely, reduce the chances of a subsequently successful criminal prosecution, and could adversely affect administrative action.

3-6. Suspect or Accused Person

Article 31, Uniform Code of Military Justice (UCMJ), and the Fifth Amendment to the United States Constitution prohibit the US Government from compelling any person to incriminate himself or to answer any question, the answer to which may tend to incriminate him, and further that he may remain absolutely silent and not answer any questions. To be admissible against him, a confession or admission of the accused must be voluntary. A statement obtained through any use of coercion (or other unlawful influence or inducement) is termed involuntary; physical violence, confinement, and interrogation to the point of exhaustion are examples of acts which may produce involuntary statements. Courts will use a "reasonable man" test to determine whether the investigator should have considered the individual a suspect and, therefore, given an explanation of rights under article 31, UCMJ. It should be noted, however, that much derogatory information from the point of view of security suitability or even loyalty is not criminal in nature; however, the explanation of rights requirements as set forth in AR 381-130 will be adhered to in those cases required by the control office. If the individual appears confused as to his rights or status, the agent should make every reasonable effort to remove the confusion. As the factors that affect a proper warning may be changed by court decision, appropriate advice should be sought on a continuing basis from a judge advocate.

a. Interrogation or Interview of a Subject, Suspect, or Accused Person.

(1) To enforce the constitutional prohibition against psychologically coerced confessions, the Congress, the Supreme Court, and the Court of Military Appeals have acted to require Special Agents to explain legal rights to all suspects and accused persons prior to questioning. Failure to give the explanation, even to a suspect who is himself a lawyer or Special Agent, will result in the exclusion of the interviewee's statements at any trial. Therefore, prior to beginning any subject interview, the Special Agent will inform the individual of the offense of which he is accused or suspected. If the Special Agent is unsure of the precise charge, he will explain, as specifically as possible, the nature of the facts and circumstances which have resulted in the Special Agent's considering the individual to be a suspect.

(2) If a suspect waives his rights, then the Government must be prepared at trial to prove beyond a reasonable doubt that the defendant understood his rights and chose to waive them voluntarily, knowingly, and intelligently. This is a greater burden than merely showing that he was "read his rights" and did not attempt to assert them. Whether the Government can sustain this burden at trial will depend largely upon the testimony and written record furnished by the Special Agent who conducted the interview.

b. Manner in Which Explanation of Rights Is To Be Given.

(1) 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 United States Constitution. A mere recitation of this explanation, however, does not assure that subsequent statements by the subject will be ad-
missible in court, as it must be shown that the suspect, in fact, understood his rights.

(2) The explanation of rights will not suffice if delivered in an off-hand or ambiguous manner. Nor should the tone of the interrogator’s voice suggest that the explanation 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 his right to remain silent or his right to counsel. Such action will be denounced by the courts as overreaching and contrary to the purpose of the explanation of rights requirement.

The same result will occur if the interrogator accidentally misstates or confuses the provisions of the explanation. Even in a purely administrative hearing, it will tend to cast Special Agent in a very unfavorable light; this, in turn, could damage his own credibility before the board. In addition, all other evidence offered will become suspect, for besides excluding illegally obtained statements, the courts may reject, and the boards are free to reject, any evidence which is not the logical product of legally obtained statements. However, 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 vitiating an otherwise proper Article 31 and fifth amendment explanation of rights.

c. The Explanation of Rights. The Special Agent will administer the following explanation of rights, making use of the parenthetical explanation when the suspect appears confused or in doubt. Any further explanations which are necessary should be given as well:

Before I ask you any questions, you must understand your rights. You are accused or suspected of _________ (offense) by/for ___________ (facts supporting offense).

(1) You have the right to remain absolutely silent. (You do not have to answer my questions and you do not have to make any statement. Your decision to remain silent cannot be held against you. If you decide to speak, but later change your mind, you can assert this right at that time and the interrogation will stop immediately. However any statement you may have made prior to stopping the interrogation may be used against you.)

(2) Any statement you make, oral or written, may be used as evidence against you in the event of a criminal trial or administrative proceeding.

(3) (a) For military: You have the right to consult with a lawyer and to have a lawyer present with you during questioning. You may hire a lawyer at your own expense, or a military lawyer will be appointed for you at no expense to you. He will be a military lawyer of your own selection if he is reasonably available. (You have the right to both a civilian lawyer at your own expense and a military lawyer at the government’s expense. Your military lawyer will either be someone you choose, provided he is reasonably available, or someone appointed who is acceptable to you.)

(b) For civilians: You have the right to consult with a lawyer before being asked any questions and to have the lawyer present with you during questioning. If you cannot afford a lawyer and want one, a lawyer will be appointed for you.

(4) Even if you decide to answer questions now without a lawyer present you may stop answering questions at any time or stop answering questions until you consult with a lawyer. (You do not have to answer any of my questions. You can answer some, and refuse others. You can stop the interrogation whenever you wish. If you tell me that you do not want to answer any more questions, I will not ask you any more questions and we will end the interview right there.) Also, you may request a lawyer at any time during questioning.

d. Explanation of Rights. If the interviewee indicates that he wishes to consult with counsel for any reason, no further attempt to question him will be made until he has conferred with counsel, or has been afforded the opportunity to do so. If he decides to waive any right, such as his right to have counsel present at the interrogation or his right to remain silent, he will be informed that he may reassert the right at any time. Under no circumstances will he be questioned until the interrogator is satisfied that the individual under-
stands his rights. An effort will be made to have him sign a “Waiver Certificate” (part I, DA Form 2820, Statement of Accused or Suspect Person). If the suspect cannot afford a lawyer, the interrogation cannot resume until he has been furnished with a qualified counsel. If the suspect refuses an appointed counsel, he must have a reasonable basis for that refusal, e.g., obvious incompetency, but he may not arbitrarily declare the counsel unacceptable.

(1) Military Suspects. If the individual is suspected of an offense under the Uniform Code of Military Justice, and is himself subject to the Code, he is entitled to be represented by an attorney at government expense, either an Army lawyer of his own choice, or if he is not reasonably available, any detailed lawyer from the local JAG office. The suspect may also retain a civilian lawyer at his own expense. If the suspect requests his own civilian lawyer, the interrogator must allow him the opportunity to retain one before continuing the interrogation. 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 his assertion of his rights to counsel.

(2) Civilian Suspects. 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 him to retain his own counsel. If he has no lawyer, the interrogator should aid him in obtaining legal counsel by providing him with the names and addresses of local agencies that provide legal services. 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, for the interrogation can only continue when the suspect is properly represented. All questions about legal representations should be directed to the local Staff Judge Advocate.

e. Understanding of Rights. The interrogator should be prepared to question the suspect about each right. Whenever possible a verbatim recording of these questions and answers should be made. If this is not possible, the interrogator should ask the suspect to acknowledge both the explanation of rights and his understanding of his rights in writing. It is highly desirable to obtain oral and written acknowledgements. With evidence of both oral and written acknowledgements, the interrogator is well prepared to rebut any charge that the suspect did not understand his rights. Appropriate questions are:

(1) Do you understand that you have the right to have a lawyer of your choice here at this interrogation to advise and assist you?

(2) Do you also understand that your right to a military counsel means a professional lawyer and not just an officer or military superior?

(3) Do you understand that the Army will provide you with a military lawyer free of charge?

(4) Do you understand that you have the right to remain silent?

(5) Do you understand that if you decide to answer questions that you may stop whenever you choose?

(6) 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?

f. The Waiver.

(1) Evidence that the suspect made a conscious and knowledgeable decision to answer questions without a lawyer (or to speak with the assistance of a lawyer) also should be obtained in writing and through the use of the following answering my questions?

(a) Do you understand each right that I have just explained?

(b) Do you have any questions about your rights?

(c) Do you want a lawyer to assist you in answering my questions.

(d) Do you want to answer my questions without the assistance of a lawyer?

(2) Any written waiver should state explicitly:

(a) I (do, do not) want counsel at this time.

(b) I (do, do not) want to make a statement or answer questions.

g. Halting Interrogation After Waiver Obtained.

(1) If, at any time and for any reason, the suspect indicates in any manner that he does not want to answer any more questions or wants to see a lawyer, the interrogation should stop immediately. No attempt should be made to persuade him to change his mind.

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

h. Evidence Obtained Involuntarily From a Suspect or Accused Person. Article 31 also prohibits any use of coercion, unlawful influence, or unlawful inducement in obtaining any other evidence from a suspect or accused. One general rule is that evidence which requires a suspect to exercise his mental faculties may not be compelled. Conversely, acts which do not require such exercise of the faculties may be compelled provided the means of coercion fall within the limits of fundamental decency and fairness. Each of these rules is often quite difficult to apply unless guidance is obtained from a legal officer or judge advocate.

i. Improper Explanation of Rights. If a suspect has been interrogated without a proper explanation of rights, it is possible to cure the defect and proceed after a valid explanation of rights; however, he must be told that his previous statement(s) cannot be used against him. If the suspect has not been told that his previous statements cannot be used against him, subsequent admissions might be the result of his belief that his earlier admissions were still of use to the Government. If the Special Agent does not know whether a prior statement was properly obtained, he should give this curative explanation of rights, and he may succeed in producing useful evidence notwithstanding the irregular procedure (para 140a, Manual for Courts-Martial, 1969 (Rev. Ed.)).

3-7. Search and Seizure

a. Search. The Manual for Courts-Martial and the fourth amendment protect individuals against "unreasonable searches and seizures of their persons, houses, papers and effects" and prescribes that this right will not be violated. The fourth amendment forms the basis for this right in our federal, state, and military court systems. An "unlawful search" is one made of a person or of his 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" means evidence from which a reasonable, prudent, and responsible individual would conclude that an offense has been or is being committed; it means more than mere suspicion, report, or good reason to suspect, and it must have been obtained legally. Any evidence found as a result of an illegal search or seizure is inadmissible in any civil or military trial and might well taint other evidence derived from the material found, thus precluding further judicial action.

b. Legal Search.

(1) General.

(a) The legality of each search necessarily depends upon all of the facts in each situation.

(b) A search may be overt or covert.

(2) Types of legal searches.

(a) Search warrant. A search conducted in accordance with the authority granted by proper search warrant is lawful. The warrant must be issued from a court having jurisdiction over the place searched.

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

(c) To avoid removal of criminal goods. A search is lawful when made under circumstances necessitating the taking of "Immediate Action" to prevent the removal or disposal of property believed on reasonable grounds to be criminal goods.

(d) Consent search. 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." Figure 3-1, provides a format which incorporates the legal requirements for consent of the owner.

(e) United States property.

1. A commanding officer having jurisdiction over the place wherein is situated property owned or controlled by the United States 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 United States or a foreign country. Such a search must also be based upon probable cause.

2. For most purposes, routine personnel security investigations and routine investigations of military or civilian personnel when entering or
CONSENT TO SEARCH

DATE: 
PLACE: 
TIME: 

I, ____________________________, fully understanding my right to refuse, do hereby voluntarily authorize Special Agent(s) ________________________________ to search my ______________________ located (at) (in) ________________________________.

I have been informed of my right to resist this search under paragraph 152 of the Manual for Courts-Martial, 1969 (Rev. Ed.) and under the fourth amendment to the Constitution of the United States of America. I am also aware that any evidence which is found may be used against me in a court of law.

______________________________

WITNESS: ________________________________

______________________________

Figure 3-1. Consent search form.

leaving military areas are not considered to be "searches" but are treated as legitimate administrative measures. Contraband (e.g., narcotics, other illegal goods, etc.) may be seized when discovered during a legitimate administrative inspection by gate guards or other personnel.

3. If possible, requests for authority to search should be in writing and should state sufficient factual information to support a conclusion that an offense has been committed and that certain property used in committing the offense, or obtained as a result of the offense, is located at
or within the place or property to be searched. Permission to search should be granted by indorsement to such request.

c. Search Procedures. The law of search and seizure must always be related to the actual circumstances; the advice of a staff judge advocate or legal officer should be obtained in any doubtful case. The following procedures however, are valid for any search:

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

(2) The Special Agent submits this evidence to the person with authority to order a search of the place or property. If the place or property is located in a civilian community in the United States, the evidence is submitted to the judge or court with authority to issue a search warrant. 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 the law of war, the evidence is submitted to a commanding officer of the US Armed Forces who has jurisdiction over personnel subject to military law or to the law of war. The evidence is submitted to a commanding officer having jurisdiction over the place where the property is located.

(3) The person with authority to order a search must find in the evidence probable cause to believe that the specified place or property contains specified objects subject to lawful seizure. If the person finds probable cause, he may then lawfully authorize the search.

(4) Having been so authorized, the Special Agent may search the specified place or property for the specified objects.

d. Civilian Search Warrants. To obtain a search warrant from a civilian court, counterintelligence personnel must establish liaison with local civilian police agencies who are authorized to request search warrants and perform the search.

e. Search and Seizure as Separate Factors.

(1) It is possible to have a legal seizure during an illegal search (e.g., the seizure of contraband is always legal, although the illegality of the search will prevent the use of such contraband as evidence) or an illegal seizure during a legal search.

(2) 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.

f. Seizure. If the search is lawful, certain objects may be seized and admitted in evidence against the suspect:

(1) Contraband. Property which is prohibited by law. Narcotics and untaxed liquor are examples.

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

(3) The tools or means by which the crime was committed.

(4) Other evidence of the crime, such as clothing.

3–8. Apprehension

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

b. Authorized individuals may apprehend persons subject to the UCMJ upon reasonable belief that an offense has been committed and that the person arrested committed the offense. This is apprehension for probable cause.

c. The authority of the Special Agent to apprehend is specified in Article 7, UCMJ; paragraph 19a, Manual for Courts-Martial, United States, (Rev. Ed.), and AR 381–103.

d. To cause the apprehension of a DOD affiliated civilian suspect, counterintelligence personnel must establish liaison with civilian police who have arrest authority. The basis for arrest by civilian police will depend on the particular jurisdiction concerned. In general, civilian police make arrests either by a warrant upon a showing of probable cause to a magistrate or without a warrant, but for probable cause, when a felony or misdemeanor is committed or attempted in their presence, or if a reasonable belief exists that the person committed the offense.

e. Incident to a lawful apprehension, the suspect’s person, clothing that he is wearing, and
property in his immediate possession or control may be searched. Any weapon or means of escape may be lawfully seized in addition to those objects specified in 3-7b(2).

3-9. Results of Unlawfully Obtained Evidence
Evidence unlawfully obtained through any of the ways covered in this section is inadmissible as evidence against the suspect or accused; any other evidence subsequently obtained as a result of this evidence is likewise inadmissible.

3-10. Unlawful Seizures
Whether the use of a particular item in evidence violates an individual's rights is usually a complex and technical determination. Advice should be obtained from the local judge advocate or as specified by the unit in its SOP. The mere fact that such an object is not related to the purpose for which the search was undertaken does not necessarily make the seizure unlawful.

3-11. Authority to Search
a. All searches, overt or covert, require prior approval from the unit headquarters or as specified by SOP.

b. Agent Reports revealing covert searches will be classified at least CONFIDENTIAL.

3-12. General
In the course of counterintelligence investigations, the Special Agent frequently finds it necessary to request a statement from a person who has personal knowledge crucial to an investigation. The best means of making an accurate and complete record of this information is the sworn statement. A sworn statement (sometimes called an affidavit) is a written statement of facts voluntarily made by a person competent to be a witness who affirms under oath that the contents of the statement are true. Counterintelligence Special Agents are authorized by Article 136(b), UCMJ, to administer the oath in conjunction with sworn statements taken in the course of their duties.

3-13. Application
a. Special Agents will request sworn statements from sources whenever credible derogatory information is given or whenever credible non-derogatory information which tends to rebut previously obtained credible derogatory information is given. Special Agents will request sworn statements from subjects, suspects, and accused persons whenever such persons are interviewed. Appropriate forms are published for this purpose. However, no special form is required to make a sworn statement admissible in evidence, but Department of the Army policy requires preparation of a sworn statement on DA Form 2820 (Statement by Accused or Suspect Person). Whenever a Special Agent prepares a sworn statement for a source or witness he will use DA Form 2823 (Witness Statement), which contains no reference to accusations, Article 31, UCMJ, or the Fifth Amendment to the Federal Constitution.

b. In some instances an affiant (or his counsel) may prefer to submit his own sworn statement following his own format. He may do so, but the Special Agent will endeavor to make certain that the statement is complete. It is recommended that the Special Agent supply the affiant with the appropriate blank forms for this purpose.

3-14. Uses for Sworn Statements
Sworn statements are requested to help Special Agents and case control officers to appraise the credibility of sources for investigative purposes and to protect the interests of sources and subjects by providing an accurate record of their interview or interrogation. Sworn statements also furnish means of persuading magistrates, US Commissioners, and commanders to authorize searches, apprehensions, or arrests. In addition, they provide loyalty adjudicators, clearance issuing authorities, and personnel officers with credible information from which to determine the loyalty and suitability of military and civilian personnel. On occasion sworn statements are used in trials to prove confessions made out of court, to refresh a witness recollection, and to assist government attorneys in impeaching defense witnesses or to support government witnesses who have been accused of telling inconsistent stories.

3-15. Contents of a Sworn Statement
A complete sworn statement normally will contain the following information:
a. The name of the person making the statement (called the “affiant”), his social security account number, military unit, or civilian address.

b. The place at which the oath affirming the statement was administered (the city and state is sufficient).

c. The date the statement was affirmed.

d. An acknowledgment, if appropriate, that a full explanation of rights was given.

e. Statements, if appropriate, showing that any decision not to exercise a legal right was made with full knowledge of the nature of the suspicion, accusation, or investigation, without any coercion, unlawful influence, or unlawful inducement.

f. An association paragraph (similar to that found in the accompanying Agent Report).

g. Relevant probative facts (the body of the statement).

h. A concluding statement (technically the “affidavit”) by the affiant, supplemented by his initials at the bottom of each page, acknowledging that he has written, read, or (if blind or illiterate) heard the statement, understands it, affirms it to be true, has approved (by initialing) all corrections, and (if not stated previously) makes the statement freely without hope of benefit or reward, fear of punishment, and without being subject to coercion, unlawful influence, or unlawful inducement.

i. Signature of the affiant.

j. A statement (technically the “jurat”) by the official administering the oath attesting that the statement was “sworn to and subscribed before me this ______ day of ________, 19____, at ________.”

k. Signature of the Special Agent administering the oath.

l. Special Agent’s authority to administer such oath (Article 136(b), UCMJ).

3-16. Explanation of Rights—To Whom Given

a. The Constitution and the Uniform Code of Military Justice require that an explanation of rights be administered to all subjects, suspects, and accused persons prior to questioning.

b. Sources, such as listed and developed character references, will be given an explanation of rights, if the sources offer information which tends to incriminate them. At that time, the interview will be suspended until a full explanation of rights has been given and a valid Waiver Certificate (part 1, DA Form 2820) has been obtained.

c. When a witness or informant confesses before he was considered a suspect, the Special Agent may have to explain in court why no explanation of rights was administered. His explanation will be satisfactory if he can clearly show that at the time of the confession:

(1) the Special Agent did not suspect the subject of a crime,

(2) the atmosphere in which he was questioned was not coercive, or

(3) that the confession came as a spontaneous outburst from the subject.

d. Elicitation of information from unsuspecting suspects by undercover agents need not be exposed by the administration of an explanation of rights as long as such elicitation was not direct questioning of the suspected offense and because they normally do not take place in a coercive atmosphere. However, in cases where it is important to gain competent evidence, the advice of a judge advocate should be first solicited, as this area of law is subject to changing technical rules.

3-17. Waiver of Legal Rights

a. If the subject, suspect, or accused person does understand his rights, the Special Agent should then specifically ask him:

(1) “Do you want counsel?”

(2) “Do you consent to being questioned?”

b. If it is desired to obtain competent evidence, the person questioned should always complete a “Waiver Certificate” (Part 1 of DA Form 2820). The Special Agent should also establish in the record of the interview (i.e. through Agent Reports, witnesses, and/or tape recordings) that the full explanation of rights was given; that it was understood by the subject, suspect, or accused person (by his own acknowledgment); and that the waiver of a legal right, if any, was made freely, with full knowledge of the charges, the consequence of not remaining silent, and with the awareness that the right or rights waived could have been reasserted at any time during the interrogation.

c. The interrogator should ask the following question of the individual prior to questioning
and will include the question in Part II, Sworn Statement, immediately following the word “oath.”

**QUESTION:** Before you make any statement I would like to ask you if you understand that the word “counsel” used in Part I, above, means lawyer or attorney or attorney-at-law and do you understand that by stating “I do not want counsel” you mean that you do not want a lawyer or an attorney or an attorney-at-law present during your questioning, even though such an attorney or lawyer would be furnished to you free of charge, and if you state “I do want counsel” it means you want a lawyer or an attorney or an attorney-at-law present during your questioning. Do you also understand that the words “military counsel” as used in Part I, above, means lawyer or attorney in the military service and not a “military superior”?

**ANSWER:**

3-18. Format

a. All sworn statements should be written in the first person. The vocabulary and grammar of the affiant should be used throughout even if it is vulgar. Parenthetical expressions, official sounding abbreviations, military-style data, and investigative jargon or capitalization (such as “fnu”, “SUBJECT”, etc.) should be avoided. This practice insures that the writing reflects the witness’ intentions and therefore it is more likely that courts and administrative agencies will give weight to its contents.

b. Sworn statements can be written in several formats, including: the narrative, the question-answer, and the combined question-answer-narrative. Sworn statements prepared by or for sources (such as listed or developed character references) usually will be written in the narrative. This technique is the least time-consuming for the Special Agent and the easiest for the source who normally is asked to complete a handwritten statement before the interview is terminated. When the source tends to be vague in his expression of crucial information, the Special Agent will employ the question-answer technique to the extent necessary to assure an accurate and complete statement.

c. In all sworn statements prepared for subjects, suspects, and accused persons, the Special Agent will use the question-answer or the question-answer-narrative format, thereby assuring a substantially verbatim record for use at subsequent adjudications and trials.

d. It is important that any statement obtained contain as much detail as possible to minimize the risk that the statement could be explained or repudiated later to avoid criminal implications.

3-19. Initials, Marks, and Margins

The initials of the affiant at appropriate places on the face of the statement insure against repudiation at a later date. By initialing the statement the affiant adopts it as his own. Typewritten statements prepared by the Special Agent should be initialed—before the first and after the last word of the statement on each page; above or beside each erasure, correction, or crossout; and at the bottom of each page. Handwritten statements need not be initialed, except where crossouts, corrections, and erasures occur. Further, to avoid charges of tampering, the Agent should type close to all margins, line out unused spaces, and draw in margins as appropriate. It is further suggested that the affiant initial lined-out areas.

3-20. Rumor, Second-Hand Information, and Potential Hearsay

Sworn statements should be requested primarily from persons who have direct, personal knowledge of the facts. If the information offered was told to the affiant by someone else, the Special Agent will attempt to obtain a sworn statement from the originator. When the Special Agent has the opportunity to assist the affiant in preparing the statement, he should tactfully attempt to have the statement distinguish between first-hand and second-hand information and state clearly the sources of all information. At the same time, the Agent should not refuse to accept sworn statements prepared by the affiant which fail to make this distinction. Inadmissible remarks can be edited out by the judge or law officer before the statement is read to the jury or court-martial. To assist other investigators and loyalty and suitability adjudicators, however, the Agent should question the affiant about each source of information and note the source in the accompanying agent report.

3-21. Opinions and Conclusions

Opinions and conclusions tend to discredit the reliability of a sworn statement. The function of a court-martial, jury, or other adjudicative board is to form its own opinion and its own conclusions from verifiable facts. Therefore, conclusions about the subject’s suitability for a “position of trust and responsibility” have no place in a sworn
statement. Similarly, speculations by the source about the subject’s possible motives, income, activities, etc., should be avoided whenever possible. Instead, the Special Agent should attempt to obtain the facts upon which such opinions are based, and persuade or guide the affiant to substitute the facts for the opinions. In this way, the fact-finders are not distracted by irrelevant conclusions and the subject, suspect, or accused person is guaranteed a fair administrative or judicial decision. Following this procedure in no way hampers the investigation; opinions and conclusions are recorded in the Agent’s Report.

3-22. Handwritten Statements
A statement taken at the time of the interview or interrogation should be in the affiant’s own handwriting (DA Forms 2820 and 2823 should be used). Nevertheless, typewritten statements are preferred for administrative convenience. Therefore, if the handwriting of the affiant is difficult to read, the Special Agent should have it typed and return it to the affiant for his signature, under oath. Once this is accomplished, the two statements should be included in the record of the investigation. Under no circumstances should the original handwritten statement be destroyed.

3-23. Statement Taken in Foreign Countries
The procedures for taking statements of US personnel outside the United States do not differ from those employed for taking statements in CONUS. When statements are taken form the nationals of a host country for use by that country as well as by the United States, the statements should conform to that country's requirements as well. In such instances it should be remembered that it is the completeness, and not the form, that determines the validity of a sworn statement under American law. A judge advocate should be contacted as to the procedures and legal limitations involved in administering an oath to foreign nationals.

3-24. Statements in a Foreign Language
When a sworn statement is taken from a person who does not speak English, an interpreter-translator must be used. He will assist in the preparation of copies of the sworn statement in each language. Both statements must include a certification by the interpreter-translator that his renditions of the affiant’s statements and the Special Agent’s questions are accurate and complete and that the interpreter-translator is competent to make the translation. An appropriate certification is: “I affirm that I am fully conversant in both the English and languages and that my interpretation and translation in preparation of this sworn statement have been accurate and complete.” The Special Agent must administer the oath of truthfulness (para 3-27) to the interpreter-translator and attest to its administration by signing a jurat (the “Sworn to and subscribed before me. . .” paragraph) which will be entered on the sworn statement following the interpreter-translator's certificate.

3-25. Oath of Truthfulness
a. Prior to asking the affiant any questions, but following the explanation and acknowledgment of legal rights, the Special Agent will administer the oath. 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, in the case of an agnostic or an atheist, be offensive.

b. If the affiant brings in a sworn statement of his own making, the Special Agent will administer the following oath: “Do you affirm that the statement you are about to sign is the truth, the whole truth, and nothing but the truth?”

3-26. Unsworn Statements
If a person refuses to make the statement under oath, the Special Agent should not attempt to persuade him to change his mind. However, the Agent may discuss the meaning of the oath and explain that there are severe penalties for false swearing or making a false official statement, and that an unsworn statement also may be used as evidence. In a loyalty action every effort should be made to obtain a sworn statement from the subject involved.

3-27. Unsigned Statements
When a person makes a oral statement under oath but refuses to sign a statement prepared from his remarks, the Special Agent should not attempt to persuade him to change his mind. The Agent should explain, however, that it is the oath, and not the signature, that makes a statement a sworn statement. Therefore, if the affiant has any reservations about the accuracy or completeness of the sworn statement he gave orally, he should consider making another statement under oath for the purpose of extending or clari-
fying his remarks. If the affiant chooses to make a supplementary sworn statement, the Agent should repeat the explanation of rights and obtain another completed waiver form. An oral confession or admission can be used in court if it is corroborated even though not sworn to or reduced to writing. It is absolutely necessary that the Special Agent make detailed and accurate notes for use as support testimony in court.

3—28. Examples

The following are examples of properly executed sworn statements.
### Statement by Accused or Suspect Person

**Place**
(Enter City and State)

**Date Prepared**

**Time Prepared**

**File Number**
(Dossier Number)

**Last Name, First Name, Middle Name**
(Self-explanatory)

**Social Security Account No.**

**Grade**
(Enter Grade or N/A)

**Organization or Address**
(Self-explanatory)

---

#### Part I - Waiver Certificate

I have been informed by (Name of Special Agent) of Military Intelligence, US Army that he wants to question me about which I am accused or suspected. He has also informed me of my rights.

I understand that I have the right to remain silent and that any statement I make may be used as evidence against me in a criminal trial.

I understand that I have the right to consult with counsel and to have counsel present with me during questioning. I may retain counsel at my own expense or counsel will be appointed for me at no expense to me. If I am subject to the Uniform Code of Military Justice, appointed counsel may be military counsel of my own choice if he is reasonably available.

I understand that even if I decide to answer questions now without having counsel present, I may stop answering questions at any time. Also, I may request counsel at any time during questioning.

**Do** (Do not) want counsel.

**Do** (Do not) want to make a statement and answer questions.

**Signature of Deponent**

**Signature of Person To Be Questioned**

---

**Interrogator:** (Self-explanatory)

**Witness:** (Self-explanatory)

---

#### Part II - Sworn Statement

I, (Enter Deponent's Name), want to make the following statement under oath:

Q: Before you make any statement I would like to ask you if you understand that the word "counsel" used in Part I above, means lawyer of attorney or attorney-at-law and do you understand that by stating "I do not want counsel" you mean that you do not want a lawyer or an attorney or an attorney-at-law present during your questioning, even though such an attorney or lawyer would be furnished to you free of charge, and if you state "I do want counsel" it means you also understand that the words "military counsel" as used in Part I above, means lawyer or attorney in the military service and not a "military superior"?

Enter appropriate phrase; e.g., "my background," "my qualification of DD Forms 98 and 398," "my association with John Jones, a member of the CPUSA," or the name of the individual or incident being investigated.

When deponent waives his right to counsel, he will strike out the word "(do)" waiving this right, and initial above these strikeovers.

Begin statement with above question and have deponent initial above the first word of the statement; above any corrections or strikeovers in the body of the statement; and above the last word of the statement.

Enter total number of pages of the statement.

---

**Exhibit**
(Leave blank)

**Initials of Person Making Statement**
(Self-explanatory)

**Page 1 of 4**

Additional pages must contain the heading "Statement of _ taken at _ dated _ continued.

The bottom of each additional page must bear the initials of the person making the statement and be initialized as "Page _ of _ pages." When additional pages are utilized, the back of page 1 will be lined out, and the statement will be concluded on the reverse side of another copy of this form.

---

Figure 3-2 Sworn statement format.
STATEMENT (Continued)

A
H
P
L

AFFIDAVIT

I. ______ (Enter Dependent's Name)

 HAVE READ OR HAVE HAD READ TO ME THIS STATEMENT WHICH BEGINS ON PAGE 1 AND ENDS ON PAGE 5. I FULLY UNDERSTAND THE CONTENTS OF THE ENTIRE STATEMENT MADE BY ME. THE STATEMENT IS TRUE. I HAVE INITIALED ALL CORRECTIONS AND HAVE INITIALED THE BOTTOM OF EACH PAGE CONTAINING THE STATEMENT. I HAVE MADE THIS STATEMENT FREELY WITHOUT HOPE OF BENEFIT OR REWARD, WITHOUT THREAT OF PUNISHMENT, AND WITHOUT COERCION, UNLAWFUL INFLUENCE, OR UNLAWFUL INDUCEMENT.

WITNESSES:

(Signature)

(NAME TYPED)

(Special Agent or if civilian, give address)

ORGANIZATION OR ADDRESS

Self-explanatory

(Signature of Person Making Statement)

Subscribed and sworn to before me, a person authorized by law to administer oaths, this ______ day of ______, 19______

City and State

(S/A Signature)

(Signature of Person Administering Oath)

(S/A NAME TYPED) (Special Agent)

(Typed Name of Person Administering Oath)

Organization or Address

Article 136(b), UCMJ

(Authority To Administer Oath)

INITIALS OF PERSON MAKING STATEMENT

(Have deponent Initial Here)

5 PAGE OF PAGES

Figure 3-2—Continued.
STATEMENT OF (Name of Deponent) Taken at (City and State), (Date) (continued).

(When additional space is needed, continuation sheets (bond paper) will be used. The above heading will appear on each additional sheet. Deponent's initials and "page__of__pages" will also be typed on each additional page as illustrated below. At the conclusion of the statement, regardless of the number of pages, the following entry will be made:)

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\}
STATEMENT BY ACCUSED OR SUSPECT PERSON
(AR 195-10)

PLACE
Presidio of San Francisco, California

DATE
2 Feb 72

TIME
1500

FILE NUMBER
BB 35 67 98

LAST NAME, FIRST NAME, MIDDLE NAME
Neuman, Alfred E.

SOCIAL SECURITY ACCOUNT NO.
458-58-5821

GRADE
CPT

ORGANIZATION OR ADDRESS
US Army Repository Group (3000), Presidio of San Francisco, California

PART I - WAIVER CERTIFICATE
I HAVE BEEN INFORMED BY Elliot A. Ness, Special Agent of Military Intelligence, US Army
THAT he wants to question me about an omission and possible falsification of an SPH
OF WHICH I AM ACCUSED OR SUSPECTED. HE HAS ALSO INFORMED ME OF MY RIGHTS.
I UNDERSTAND THAT I HAVE THE RIGHT TO REMAIN SILENT AND THAT ANY STATEMENT I MAKE MAY BE
USED AS EVIDENCE AGAINST ME IN A CRIMINAL TRIAL.
I UNDERSTAND THAT I HAVE THE RIGHT TO CONSULT WITH COUNSEL AND TO HAVE COUNSEL PRESENT
WITH ME DURING QUESTIONING. I MAY RETAIN COUNSEL AT MY OWN EXPENSE OR COUNSEL WILL BE APPOINTED FOR
ME AT NO EXPENSE TO ME. IF I AM SUBJECT TO THE UNIFORM CODE OF MILITARY JUSTICE, APPOINTED COUNSEL
MAY BE MILITARY COUNSEL OF MY OWN CHOICE IF HE IS REASONABLY AVAILABLE.
I UNDERSTAND THAT EVEN IF I DECIDE TO ANSWER QUESTIONS NOW WITHOUT HAVING COUNSEL PRESENT,
I MAY STOP ANSWERING QUESTION AT ANY TIME. ALSO, I MAY REQUEST COUNSEL AT ANY TIME DURING QUESTIONING.
I (DO) WANT COUNSEL.
I (DO) WANT TO MAKE A STATEMENT AND
ANSWER QUESTIONS.

INTERROGATOR: (Signature)

WITNESS: (Signature)

Elliot A. Ness, 116th MI Group

PART II - STATEMENT
I, Alfred E. Neuman, Want to make the following statement under OATH:

Q: Before you make any statement I would like to ask you if you understand that the
word "counsel" used in Part I above, means lawyer or attorney or attorney-at-law and
do you understand that by stating "I do not want counsel" you mean that you do not
want a lawyer or an attorney or an attorney-at-law present during your questioning,
even though such an attorney or lawyer would be furnished to you free of charge, and
if you state "I do want Counsel" it means you want a lawyer or an attorney or an
attorney-at-law present during your questioning. Do you also understand that the words
"military counsel" as used in Part I above, means lawyer or attorney in the military
service and not a "military superior"?

A: Yes, I understand that the word "counsel" means lawyer or attorney-at-law, and that
I may have a lawyer present at my questioning if I so desire.

Q: Please state your full name, grade, service number, organization, duty station, and
place of birth.

Francisco, California, born 22 January 1945 in San Francisco.

Q: Captain Neuman, it is the policy of the Department of the Army to allow the subject
of a personnel security investigation every reasonable opportunity to refute, explain,
or mitigate the effect of derogatory information that has arisen during the course of
an investigation. Information has been received that you were arrested on 11 November
1968 in San Francisco, California, and charged with responsibility for a hit-and-run.

EXHIBIT

INITIALS OF PERSON MAKING STATEMENT

ADDITIONAL PAGES MUST CONTAIN THE HEADING "STATEMENT OF TAKEN AT DATE
CONTINUED." THE BOTTOM OF EACH ADDITIONAL PAGE MUST BE INITIALED AS "PAGE OF PAGES.
WHEN ADDITIONAL PAGES ARE UTILIZED, THE BACK OF PAGE 1 WILL BE LINE
ED OUT, AND THE STATEMENT WILL BE CONCLUDED ON THE REVERSE SIDE OF ANOTHER COPY OF THIS FORM.
clement. You did not list this arrest on your Statement of Personal History, DD Form 398, dated 10 November 1970. The purpose of this interview is to determine why you omitted this arrest. Do you understand the purpose of this interview?

A: I do.

Q: I now show you a copy of DD Form 398 dated 10 November 1970. Do you recall preparing this form?

A: Yes, I do.

Q: Is this your signature on this form?

A: Yes.

Q: Why did you not list your 11 November 1968 arrest?

A: It is true I was arrested in 1968 for hit and run. However, the charges were dropped. The case never went to trial. Three days after I had been arrested, the police decided I was telling the truth when I said I did not realize I had hit someone. As it turned out, the victim was a drunken derelict who had walked into the right rear side of my car as I was making a right hand turn on a dark rainy night. The police even found a witness who said that the victim walked into my car and that I was not speeding.

Q: Are you aware of the fact that question 18 of DD Form 398 asks if you have ever been detained or arrested, regardless of whether or not you were convicted or ever went to trial?

A: That is not the way I interpreted the question, especially since the arrest was really not justified and I never spent any time in jail.

Q: Is there anything which you would like to add to this statement?

A: No.

AFFIDAVIT

I, Alfred E. Neuman——— HAVE READ OR HAVE HAD READ TO ME THIS STATEMENT WHICH BEGINS ON PAGE 1 AND ENDS ON PAGE 2, I FULLY UNDERSTAND THE CONTENTS OF THE ENTIRE STATEMENT MADE BY ME. THE STATEMENT IS TRUE. I HAVE INITIALED ALL CORRECTIONS AND HAVE INITIALED THE BOTTOM OF EACH PAGE CONTAINING THE STATEMENT. I HAVE MADE THIS STATEMENT FREELY WITHOUT HOPE OF BENEFIT OR REWARD, WITHOUT THREAT OF PUNISHMENT, AND WITHOUT COERCION, UNLAWFUL INFLUENCE, OR UNLAWFUL INDUCEMENT.

Alfred E. Neuman
(Signature of Person Making Statement)

Subscribed and sworn to before me, a person authorized by law to administer oaths, this 2 day of February, 1972, at The Presidio of San Francisco, California.

Elliot A. Ness
(Signature of Person Administering Oath)

Organization or Address

INITIALS OF PERSON MAKING STATEMENT AEN

Page 2 of 2 Pages

Figure 3-3—Continued.
I first met CPT Robert H. Humphrey in May 1965 when I was assigned to the Fort Huachuca Security and Plans Office. He was the Plans Officer for the Office. We worked together until August 1968 when he was reassigned somewhere in Asia. I have not seen him since and we have not communicated in any way. While he was stationed at Fort Huachuca, we visited in each others homes on an alternate weekly basis. One day in January 1968, I saw Humphrey placing classified defense information, to include SECRET material, into his briefcase. I questioned the necessity of taking classified defense information home, and I pointed out that it was in violation of post regulations. Humphrey told me that he frequently worked on plans at home so that he would not have to work at the office at night, but Humphrey assured me that he secured the material in his home so that no unauthorized personnel could read or obtain copies of it. I did not repeat this to our superior, COL William A. Custer, Chief, Security and Plans, because I was confident that Humphrey was careful with the handling of classified defense information while it was out of the office. I also knew that Humphrey's hobby was photography with miniature cameras and that he maintained his own darkroom in a storage closet of his quarters. Additionally, I was aware that in August 1968 when Humphrey was departing from Fort Huachuca that the classified cage easily cleared him and that he had no outstanding documents charged to him. I am unaware of any altered certificates of destruction during any period in which he was the Destruction Officer for the Fort Huachuca Security and Plans Office. I know of no foreign friends or relatives that he may have. I consider Humphrey to be an honest, loyal officer in the US Army.
AFFIDAVIT

Leonard D. Fink

I, Leonard D. Fink, have read or have had read to me this statement which begins on page 1 and ends on page 2. I fully understand the contents of the entire statement made by me. The statement is true. I have initialed all corrections and have initialed the bottom of each page containing the statement. I have made this statement freely without hope of benefit or reward, without threat of punishment, and without coercion, unlawful influence, or unlawful inducement.

WITNESSES:

William R. Cop

Subscribed and sworn to before me, a person authorized by law to administer oaths, this 13th day of January, 1972, of Fort Huachuca, Arizona.

Glenn F. Beach

ORGANIZATION OR ADDRESS

115th MI Group

INITIALS OF PERSON MAKING STATEMENT

WITNESSES:

Glenn F. Beach

ORGANIZATION OR ADDRESS

Article 136(b), UCMJ

Signature of Person Administering Oath

Typed Name of Person Administering Oath

Authority To Administer Oaths

FM 30-17

Figure 3-4—Continued.
CHAPTER 4

BASIC INVESTIGATIVE TECHNIQUES AND PROCEDURES

Section 1. INTRODUCTION

4—1. General

"Investigation" is a duly authorized, systematized, detailed examination or inquiry to uncover facts and determine the truth of a matter. The purpose of a counterintelligence investigation is to supply the commander with sufficient factual information on which to base an adjudicative decision or to initiate action to insure the security of his command. Counterintelligence investigations utilize basic investigative techniques and procedures similar in many respects to those employed by criminal investigators of law enforcement agencies. The purpose of criminal investigations, however, is to determine the facts of an alleged crime and to apprehend the offenders. Counterintelligence investigations are aimed at the detection, prevention, and/or neutralization of actual or potential threats to the security of the command and the Army, regardless of whether criminal activity is involved. Although prosecution of the offenders may be the natural consequence of some counterintelligence investigations, the primary objective is the security of command. Many operations of counterintelligence units must be coordinated carefully with those of military police investigative units and other intelligence and security agencies, to preclude the operations of one agency having a negative effect on, or compromising the operations of, another.

4—2. The Investigative Plan

An investigative plan must be formulated at each operational level down to and including the level of the individual Special Agent. The purpose of the investigative plan is to define information required and pertinent aspects to be considered and to preclude unnecessary investigative effort. The investigative plan will vary in scope and detail from one at control office or MI group headquarters, which may outline the plan for an entire or major part of an investigation, to a simple plan of a regional or resident office involving only one phase or lead of an investigation. The plan of an individual Special Agent, for example, may be no more than consideration of the approach to a single interview. An investigative plan should include as many of the following considerations as are applicable:

a. Reasons for, or purpose of, the investigation.
b. Phases or elements of the investigation which have been assigned.
c. Whether the investigation is to be conducted overtly or discreetly.
d. Priority of the investigation and time permitted for completion.
e. Restrictions or special instructions.
f. Information provided, including information from the unit or office files.
g. Definition of the problem.
h. Methods and sources to be used.
i. Coordination required.

The investigative plan is updated as warranted by new developments and the continuing analysis of results.

4—3. Basic Investigative Techniques

The following basic techniques are employed as appropriate in all areas of operation and in all types of investigative activity:

a. Records Examination. An examination of the records is made to locate, gain access to, and extract or copy pertinent data from diverse official and unofficial documents and records for the production of factual data. Records are also used as a source of leads for further investigation.
b. Interview and Interrogation. Direct or indirect questioning of individuals is made for the purpose of obtaining information.
c. Surveillance. Surveillance in counterintelligence operations may be employed for the purpose of providing protection or for the collection of information, evidence, or leads. This technique is expensive in terms of time and manpower; consequently, it should be applied judiciously—generally only when required to produce results not obtainable by other means.

d. Raids and Searches. Raids and searches are seldom employed by counterintelligence units except in areas of hostilities. However, the need cannot always be anticipated and the Special Agent must have a basic knowledge of the technique and planning involved.

e. Collection and Handling of Evidence. Although the results will not often be presented in court, care must be taken to ensure that evidence collected is handled in such a manner as to make it admissible in the courts. If the evidence has been properly handled, it will also be usable by administrative boards.

Section II. RECORDS EXAMINATION

4—4. General
The systematic employment of records examination is particularly adaptable and important to the broad scope of most counterintelligence investigations. The full exploitation of records examination as an investigative tool is dependent upon several factors which must be considered by the Special Agent:

a. Types of Records Available. The counterintelligence specialist must know what, where, by whom, and for what purpose records are maintained throughout the area in which he is operating. The initial orientation of a Special Agent, upon his assignment to an operational unit, should stress thorough familiarity with records which can be of assistance in investigations.

b. Methods of Gaining Access to Records. Most records will be available to the Special Agent on an official request basis. In some cases, however, access will be contingent upon the ability of the investigator to obtain discreet cooperation of the custodian of the records. Such cooperation will be enhanced by mature, professional conduct and attituded, effective liaison, and mutual assistance. If all efforts to obtain the desired information fail it must be recognized that such information or records are not obtainable by a subpoena if a legal proceeding has not been initiated. A search warrant could compromise an investigation even if the required probable cause, in the legal sense, could be shown. Consequently, there will be occasions when documentary information or evidence will have to be obtained through other investigative means.

c. Reliability of Recorded Data. The possibility of intentional deception or false information in both official and unofficial records must always be considered. The fact that data is recorded in some documentary form does not in itself insure its reliability. Many recorded facts, particularly items of biographical data of interest in complaint-type and personnel security investigations, are merely repetitions of unsubstantiated information provided by the subject himself. Reliability of records will vary considerably according to the area, the status of the agency or organization keeping the records, and many other intangible factors. For example, records to be found in highly industrialized Western Europe will be more extensive and far more reliable than those of underdeveloped areas of Southeast Asia. Until experience with a certain type of record has been sufficient to establish a basis for evaluating their reliability, it is necessary to treat information from these records with skepticism.

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

e. Value of Negative Information. In counterintelligence investigations, for example, the absence of a record is often just as important as the existence of a record. This is especially important in the investigation of biographical data furnished by the subject of a complaint-type investigation. Another example is the systematic and meticulous examination of records to confirm or refute a suspect's story is very often the best means of breaking and enemy intelligence agent's cover story.

4—5. Types of Records of Counterintelligence Interest
The types of records and amount of detail of their content will vary markedly with the area of operation. Regardless of the area, it is important
for the Special Agent to be aware of the types of records he may be able to use in the conduct of investigations. The following are some of the major types of records which often will be of value for information or for leads.

a. Police and Security Agencies. Local, regional, and national police agencies of most nations maintain extensive personality files on criminals, suspects, victims, and other persons who have come to the official attention of police in connection with some actual or alleged criminal activity. Police interest in precise descriptive details, often including photographs and fingerprint cards, makes police records particularly valuable and usually more reliable than comparable records of other agencies. Police and security agency files are usually divided into subcategories; it is important for the Special Agent to become familiar with the records system concerned to insure that all pertinent files have actually been checked.

b. Intelligence Agencies. Because the reliability and validity of records checks with allied intelligence agencies will often depend to a large degree on the personal relationship between the counterintelligence representative and the custodian of the records of interest, such examinations normally will be the assigned responsibility of a liaison officer. This may also be necessary with other agencies when the volume of records examinations dictates the need for a single representative of the counterintelligence 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 of routine interest who are to be checked.

c. Vital Statistics. The recording of births, deaths, and marriages is mandatory in nearly every nation, either by national or local law. This information may only be maintained in family journals or Bibles in newly developing countries or in the case of very old records. In any case, confirmation of such dates may be important in many types of investigations. The records sought may be filed at local level, as is usually the case in overseas areas, or they may be kept at state or regional level, such as with state bureaus of vital statistics in the United States. Rarely will original vital statistics records on individuals be maintained centrally with a national agency.

d. Residence. Some form of official registration of residence 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 special separate police file. Residence directories, telephone books, and utility company records may also be used. In other countries, the village chief may maintain these records which may double as a record of vital statistics reflecting births, marriages, and deaths.

e. Education. Both public and private schools at all levels, from primary grades through universities, will have records which may serve for purposes of background verification. The school yearbook or comparable publication at most schools will contain a photograph and brief resume of the activities of each graduating class member, a record of value both for verification and as an aid to locating leads. Registrar records normally contain a limited amount of biographical data and a detailed account of academic activities.

f. Employment. Official and Business records related to employment of individuals may be of value.

(1) Personnel records. Personnel records usually contain information on dates of employment, positions held, payment received, efficiency, reason for leaving, attendance record, special skills, and biographical and identifying data. Access to such records for the Special Agent will be relatively simple in the United States 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.

(2) Unemployment and social security records. Depending upon the area of operation, there may be either local, regional, or national offices for the administration of unemployment and social security programs. Records of these offices often will contain extensive background material on individuals, but in most cases these data will represent unsubstantiated information provided by the applicant and cannot necessarily be regarded as confirmation of other data obtained from the same individual. It must be noted, however, that the records of the US Social Security Administration can only be obtained by the Department of Justice by written request in cases involving high level security investigations.

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

h. International Travel. A system of access to records of international travel is especially important to counterintelligence operations in overseas areas. Records of interest 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 (e.g., border police) files. Records of foreign travel of US citizens are maintained by the State Department and such information is available by means of a National Agency Check in accordance with AR 381-130.

i. Military Service. Records of current and past members of the armed services of most nations are detailed and are usually accurate:

(1) US records. Counterintelligence specialists will encounter no difficulty in obtaining access to US military service records on an official request basis. If a serviceman 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:

(a) For those personnel who have changed branches of service, the control office will need the man's former service number, social security account number, full name, and date and place of birth.

(b) When an individual has had a break in service, his field 201 file is retired, and to obtain it for review, the control office will need the individual's full name, and any former service numbers.

(c) In addition, The Adjutant General's Office, 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 status as a commissioned or warrant officer. This would, however, be the exception rather than the rule.

(d) Army hospital records which have been retired are filed by hospital, by name; consequently, the hospital name and year will be required.

(2) Foreign records. Access to foreign military records in overseas areas may be very difficult. In cases where it is not possible to arrange for examination of official records, leads or pertinent information may be obtained from unofficial unit histories and similar documents which have been published commercially and also from files on various veteran organizations. Since 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 suspected enemy agents. Special efforts may be made to locate some form of records which will either confirm or deny an individual's service in a particular unit or the existence of the unit at the time and place he claims to have served. Order of battle and personality files of various intelligence services also may be helpful.

j. Miscellaneous Organizational Affiliation. Many organizations maintain records which may be of value to a particular investigation. Examples are labor unions, social, scientific, sport groups, cultural and subversive organizations. Although it is important for the Special Agent to consider such organizations when seeking sources of information, he must be thoroughly familiar with the organization before attempting to exploit it. Organizations are often established as front groups or cover vehicles for hostile intelligence operations.

4-6. Access to Records

Having determined which records may include information pertinent to an investigation, the Special Agent must select the best means of gaining access to the records for purposes of examining or copying. In general, access to records will be accomplished by the following methods:

a. Official Inquiry. The Special Agent must contact the custodian of the records; identify himself as a Special Agent of Military Intelligence, United States Army, using his credentials; state the purpose of the inquiry; and ask for any information available. This procedure is most com-
monly employed in personnel security investigations, but it may be employed in certain phases of complaint type investigations.

b. Liaison. This process involves reciprocal cooperation between the agency whose records are of interest and the unit. Such liaison may include authorization for the liaison representative to arrange for records checks on an exchange basis within limitations imposed by higher headquarters. Liaison of this type normally will be the responsibility of a designated liaison officer, or it may be an additional duty for counterintelligence specialists.

c. Check of National Agencies. The records of national agencies in the United States are checked by forwarding a request for a National Agency Check through channels on DD Form 1584. Normally, these checks will have been initiated by the control office concurrently with assigning the investigative tasks to subordinate levels. Results of such checks, when they have a bearing on the investigative tasks being conducted at the operational level, will be forwarded through channels to the investigating officer.

Section III. INTERVIEWS

4–7. General

The interview is a form of direct interrogation used to extract information from an individual by questioning. Use of the word “interrogation” in conjunction with criminal and intelligence activities has resulted in a generally accepted connotation implying use of authority and application of subterfuge and psychological pressures. The general solicitude for the interviewee and the pleasant atmosphere of the normal counterintelligence interview are missing in an interrogation, except as they may be phases of a planned interrogation technique. The distinction between “interview” and “interrogation” is at times difficult. In some instances, e.g., interviews of walk-ins or witnesses, the hostility of a subject may necessitate the application of interrogation techniques by the Special Agent. Differentiation between the two, however, is academic provided there is adherence to legal and other requirements. In counterintelligence operations, the interview is used extensively in but not limited to, personnel security investigations (PSI). In certain instances, it may be necessary to conceal the true purpose of an interview or to obtain information without the subject becoming aware that an “interview” is taking place. Techniques for interviewing an unwitting source are discussed in paragraphs 4–19 through 4–22. The purpose of a interview as part of a PSI is to determine the loyalty, trustworthiness and the suitability of an individual by questioning people acquainted with the person. In this manner, an objective and composite picture of a person may be obtained. No single source of information can satisfy the requirements of such an investigation. Personnel security investigations constitute the majority of counterintelligence investigations, and a number of interviews are conducted in conjunction with each PSI.

4–8. Preparation for an Interview

Prior to an interview, the Special Agent must study carefully all the background information available on the case. In a PSI the subject of the investigation will have submitted a DD Form 398 (Statement of Personal History). This document is the initial source of leads; it may give an indication of the relationship between the listed references (prospective interviewees) and the subject, and it may assist in creating a mental picture of the subject—an invaluable aid in formulating a line of questioning for an interview. Often an interview will be based on a DD Form 339 (Lead Sheet), which normally contains less background information. Other sources of information, concerning both the subject and the prospective interviewee are unit files, local and Federal law enforcement agency files, telephone books, and city directories. It is frequently desirable, and necessary in critical cases when indications of the credibility of an interviewee are needed, that something about the interviewee be learned. In addition to files and records, the interviewee’s neighborhood, class of housing, condition of the home, and occupation or position may give a general, but fallible, indication of the personality of the interviewee. A telephone call to arrange an appointment with a prospective interviewee is a courtesy often advantageous to the investigator. The Special Agent’s final preparatory step is the formulation of a tentative plan for questioning the interviewee.
4–9. The Approach

The approach to an interview is simply an application of the social code of polite behavior, together with certain investigative requirements.

a. Identification of the Interviewee. The Special Agent should first determine that he is talking to the right person. The full name of the interviewee must be used to preclude all possibility for error.

b. Identification of the Special Agent. The Special Agent may have introduced himself by telephone, but he must again introduce himself as a Special Agent of Military Intelligence and present his credentials for the inspection of the interviewee.

c. Identification of the Subject of Investigation. The Special Agent must identify the subject of investigation to ascertain that the interviewee is or was, in fact, acquainted with the subject.

d. Statement of Purpose of the Interview. The Special Agent must explain to the interviewee the purpose of the interview. Some people are inclined to look with suspicion on all investigators. The patient explanation by the Special Agent of the purpose and importance of the interview and the need for the interviewee's cooperation is generally sufficient to allay suspicion and forestall any reluctance to provide information.

e. Privacy of the Interview. The Special Agent should insure, to the extent conditions permit, that the interview will not be interrupted or overheard. He should also emphasize the Army policy limiting dissemination of details of a PSI.

f. Confidential Nature of the Interviewee's Statements. The Special Agent should inform the interviewee that his having been interviewed and the matters discussed are regarded by the Army as official Army business and should not be discussed by the interviewee with other persons.

g. Establishing and Maintaining Rapport. The foregoing steps provide a means by which the Special Agent may establish rapport with the interviewee before beginning the interview proper. Rapport creates mutual confidence and cooperation between the interviewee and the Special Agent. Important to good rapport are proper dress, a pleasant voice, a courteous demeanor, and a professional manner. The burden for maintaining rapport throughout the interview rests with the Special Agent. Normally an interview will take place in the interviewee's home or place of work, where he is under no official compulsion to furnish the information sought. Topics found to be of mutual interest may be used by the Special Agent to assist in establishing rapport, but caution must be exercised to prevent the interview from becoming a mere casual conversation.

4–10. The Interview Proper

Once the interviewee has indicated his willingness to cooperate, the Special Agent must establish the area of knowledge through questioning. The area of knowledge consists of: when the interviewee and subject first met; under what circumstances; when interviewee and subject last met; under what circumstances; the period of closest association; the type of association; frequency of contact; and if there has been any communication between them. This information will also aid the Special Agent in formulating questions on the subject's loyalty, integrity, discretion, and moral character. The Special Agent now must explore all aspects of the subject's background to the knowledge of the interviewee, which are pertinent to the investigation. He must be constantly alert for leads to other persons not listed by the subject as references. If the interviewee is or was an employee or coworker of the subject, attention is focused on the subject's efficiency, initiative, and ability to get along with fellow workers and subordinates, and on his honesty, reliability, and general character. If the interviewee is or was a neighbor of subject, the subject's general reputation and that of his family, his leisure time activities, morals, and personal habits may be discussed. Concentration on some points does not imply exclusion of others. Information which will assist in establishing subject's loyalty, trustworthiness, and suitability must be sought. Following is a tentative checklist which may be useful as a general framework for an interview and a basis for discussion:

Birth of subject Date and place, with particular attention to origin.

Education Names and addresses of institutions; dates of attendance, academic records, and degrees received.

Employment Names and addresses of employers and dates of employment; names of immediate superiors and coworkers; nature of duties; quality of performance; reason for departure from job.

Technical skills Education and circumstances of development.
Interests  Hobbies and avocations.
Temperament  Emotional stability, natural inclinations, and idiosyncrasies.
Moral character  Personal habits, particular virtues and faults, illegal use of narcotics, and excessive consumption of alcohol.
Mental ability  Inherent talent, intellectual developments, general alertness.
Loyalty  Adherence to principles of the Constitution and to laws of the nation; reaction to foreign ideologies.
Integrity  Uprightness of moral character and strength of convictions.
Discretion  Speech and behavior, judgment, and self-control.
Reputation  Personality, character, and popularity.
Record  Appropriate police authorities and other agencies such as credit bureaus.
Family background  Origin of parents, relatives abroad, general reputation.
Association  Male and female friends, business or other associates, favorite haunts.
Organizations  Membership, active participation, position, professional societies, character of organization, financial contributions, persons for membership, awareness of aims of organization.
Leads  Names and addresses of persons acquainted with various phases of subject's background; impartial sources of information not listed by subject as references.
Recommendation  Interviewee's overall opinion of subject's qualifications for a position of responsibility and trust; questions concerning religious beliefs, racial matters, politics, labor affiliations, or personal and domestic matters should be avoided 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.

4-11. Important Precepts

a. Be Professional in Approach. A Special Agent, as a representative of Military Intelligence should always be dressed in accordance with his assigned duty, courteous in manner, and efficient in the execution of his duty.

b. Be Specific in Questions. General questions should be avoided since they are usually confusing. The Special Agent should pinpoint specific information desired.

c. Determine Reasons for Interviewee's Opinions. When the interviewee states, for example, that he considers the subject to be an indiscreet person, he should be requested to cite specific incidents to support his opinion. If he claims the man is a drunkard, his concept of the term should be clearly defined and his statement should be substantiated by pertinent facts.

d. Be Logical. The Special Agent should analyze point by point each phase of the subject's background. If the interviewee presents information in a haphazard manner, the Special Agent must attempt with tact to guide the discussion into a logical pattern.

e. Get All Pertinent Information the First Time. The conscientious Special Agent cannot tolerate gaps in his report, and he should get all the facts the first time; however, the Special Agent must fill any gaps in his report even if it means returning for another interview.

f. Be Interested in the Interviewee. The Special Agent must maintain an attitude of interest no matter how often the information he is receiving may have been repeated by various persons.

g. Do Not Discuss Official Information. In many cases, the interviewee expresses curiosity about the Special Agent's position and duties. The interviewee may want to know additional details about the purpose of the investigation or about information received from other sources. These are matters which cannot be disclosed due to their official nature, and the Special Agent must decline to answer inquiries with tact.

h. Keep Notes to a Minimum. It is preferable to take notes only on pertinent points of the interview, with particular attention to names, addresses, dates, and direct quotations of significance. If the Special Agent feels he should amplify his notes, he can make the necessary elaboration as soon as possible after the interview.

i. Remember Leads. It is understandable that persons listed as references by the subject of investigation normally will paint a highly favorable picture of the subject and his qualifications. In a search for objective information the Special Agent must also consult individuals (throw-offs) whose names were not provided by the subject.
who are identified as associates of the subject. Names, locations, and associations of such persons with the subject should be obtained during interviews of references or developed sources.

j. Leave a Good Impression. Regardless of the nature of the reception by the interviewee, the Special Agent should be courteous. When the Special Agent encounters hostility, he should try to dissipate it by maintaining a courteous but businesslike manner, tactfully citing reasons for the interview. He should express his appreciation for the interviewee's time and courtesy.

4–12. Interviews of Subjects of Counterintelligence Investigations

When authorized by proper authority, the subject of a PSI or of a CTI may be interviewed (AR 381–130). In all interviews of subjects of a counterintelligence investigation where the subject is accused or suspected of violating the law, the subject must be properly advised of his rights under the provisions of the Fifth Amendment to the Constitution of the United States or of Article 31 of the Uniform Code of Military Justice and of his right to counsel. It is emphasized that questions concerning religious beliefs, racial matters, politics, labor affiliations, or personal and domestic matters should also be avoided in subject interviews; however, when such information has a direct bearing on the investigation the Special Agent will phrase and time his queries so as to establish clearly that they are relevant to the investigation.

a. Subject's Right to Counsel. A suspected or accused subject has the right to legal advice at any time prior to, during, or following the interview (3–6).

b. Preparation for the Subject Interview. The subject shall be contacted and informed of the precise reason for the interview. He will be advised that the interview offers him the opportunity to refute questionable and/or misleading information or circumstances; to provide information not otherwise obtainable; or to remain silent, neither affirming nor denying the information. If the subject expresses a willingness to be interviewed, arrangements should be made for the time, date, and place of interview. Should the subject refuse to be interviewed or to answer pertinent questions, this refusal must be made a matter of official record by the Special Agent in verbatim form. The Special Agent must accumulate all available information and all pertinent leads before the conduct of the interview. Questions for each interview will be carefully preplanned, with the advice and assistance of superiors. The subject matter of the interview should be reviewed carefully to insure that only information specifically authorized by the control office is released to the subject during the interview. Under no circumstances will the subject be allowed access to any portion of his intelligence file. When directed by Department of the Army, or when, from facts available, it is considered likely that a recommendation for removal or elimination will result, verbatim transcripts will be made of the interview or of any oral statements. There is usually no obligation to furnish the interviewee with a copy of the transcript or recording or of a statement made by him, but he will be permitted to inspect the official transcript of his interview of statement. The Special Agent must then explain to him that, if he is called to appear before a field board of inquiry or a civilian security hearing board, a copy of the interview will be provided on his request. If the subject participates in the interview or signs a transcript or statement conditional upon obtaining a copy of same, a copy will be furnished, unless restrictions of AR 380–5 on the release of classified information apply. The copy furnished the subject will not bear a protective marking but should 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."

c. Precepts. The Special Agent acts as a representative of the US Army. His every statement, question, or contact will be regarded by the subject as part of the official proceedings, whether so intended or not. There will be no off-the-record or unofficial phases in the interview. Special Agents will make no promises or commitments to the subject which are beyond their authority to fulfill. Special Agents will avoid statements or representations which might be misunderstood and comments which might be construed as expressions of opinion or advice to the subject concerning his past, present or future actions. Special Agents will not argue with subjects or express personal viewpoints on any matter.

d. Female. When the subject to be interviewed is female, female witnesses must possess the appropriate security clearance. Any immoral or abnormal behavior allegations by the WAC must be referred to the WAC commander for action. In the absence of a WAC commander, such allega-
tions must be referred to the command WAC advisor. If personal questions are to be asked that may prove to be embarrassing, the female should be so warned in advance (para 4—17d(3)).

e. Steps of the Interview. The Special Agent conducting a subject interview should take the following actions in the sequence listed:

1. Dictate identifying data into the tape recorder prior to the subject's arrival. Turn off the machine.
2. Identify and welcome subject, identify self, and present credentials.
3. Explain the general purpose and confidential nature of the interview.
4. Obtain subject's permission to record the interview, explaining that the recording will facilitate the preparation of a written transcript of the interview which subject will have an opportunity to review, correct, and sign under oath.
5. Turn on the tape recorder. (If the subject objects to the tape recorder, (e.g., "Those machines make me nervous") but is willing to proceed without the tape recording, the Special Agent should proceed taking verbatim notes. Lack of a tape recording is an administrative inconvenience, but will not unduly hamper the taking of the Sworn Statement and the preparation of the Agent Report.)
6. Ask the subject to state, for the record, his name, rank, social security account number, and other identifying data as appropriate.
7. If appropriate, administer a full explanation of rights as outlined in paragraph 3—6.
8. If the explanation of rights was given, request subject complete "Waiver Certificate" (part I, DA Form 2820) on which he acknowledges receipt of the explanation of rights and decides to exercise or waive his rights to remain silent and to consult counsel.
9. If the subject chooses to waive his right to remain silent, ask him if he is willing to take the oath. (If he is not, ask him if he is willing to answer questions or make a statement without taking the oath. If he is, remind him that the statements and answers still can be used as evidence against him. If he is still willing to be interviewed, proceed.)
10. Administer the oath in accordance with paragraph 3—27.
11. Conduct the interview using prepared questions designed to elicit narrative answers. (12) When appropriate, ask the subject if he is willing to submit to a polygraph examination.
13. If appropriate, obtain a handwritten sworn statement before terminating the interview.
14. If appropriate, make arrangements for obtaining the subject's signature on a typewritten sworn statement.
15. Thank subject for his cooperation, remind him that his statements will be held in confidence and used for official purposes only.
16. Terminate the interview.

4—13. Interviews of "Walk-Ins" or Volunteers

a. General. Persons who volunteer information of intelligence interest usually do so for some personal motive. When interviewing such persons, the Special Agent must consider the source's motive (nationalism; personal gain; protection of self, family, and belongings; vindictiveness; or revenge). The source's motive(s) may be invaluable in evaluating the information or in determining the nature and extent of his knowledge. Motivation may not always be known, and may be other than that stated by the source. The Special Agent's primary concern is to obtain all information of both intelligence and counterintelligence value. If, however, the source volunteers information which is not within the jurisdiction of Military Intelligence, the source will be referred to the local police or local office of the FBI. If the source refuses such referral, the information will be obtained and immediately furnished to the proper office. Upon request, the identity of a source will be protected. This procedure will also apply to anonymous telephone callers or written messages.

b. Method of Interview. Differences in types of information and in motivation dictate the need for varied techniques. A story of an incident cannot be examined in quite the same manner as a story involving a subversive organization. A reluctant source will require a different technique from a willing source. Despite these differences, the following steps in the order given are basic to the interview of sources volunteering information:

1. Put the source at ease. The Special Agent's initial attitude frequently affects the success of the interview. The atmosphere should be pleasant; the Special Agent should be courteous
but professional. Effort should be made to avoid taking up more of the source's time than necessary. Care must be exercised to prevent compromising the source by indiscreet questioning in the presence of others.

(2) Let the source tell his own story. The source should be encouraged to tell his story in his own way. Premature questions may be disconcerting or may reveal the Special Agent's suspicious attitude, thus alarming the source and causing him to limit his information to vague generalities. If the source strays too far from the basic story, the Special Agent should tactfully steer him back to the main topic. Throughout this first narration by the source, the Special Agent should make mental notes of the salient points to guide him in the subsequent review of the story.

(3) Review the story and take notes. Once the source has completed his basic story, he generally has little reluctance to answering specific questions on the details. Given the assurance that his information will be kept in strict confidence, he will now be less apprehensive of notetaking. The story should now be reviewed critically in its entirety. Disparities, contradictions, and gaps in the story must be clarified. Every lead must be noted accurately.

(4) Obtain background information. To assist in the evaluation of the source's information, something must be known about the source himself. The source's identity, his origin, past activities, present and past addresses, occupation, interests, and motives are pertinent facts which may throw light on his reliability.

(5) Develop secondary information. The source's story and background frequently indicate that he may have further information of significant intelligence interest.

(6) Termination of the interview. When the Special Agent is certain the source has no further information, he should close the interview in a manner calculated to leave a favorable impression. If future contact with the source is a possibility, at least tentative arrangements should be made. The Special Agent should be sure to express his appreciation.

c. Precepts. In preparing for and conducting an interview of volunteers, the Special Agent should—

(1) Check, or initiate check of, the files of his unit for possible information on the source.

(2) Attempt to make arrangements to avoid interruption.

(3) Adapt himself to the source's intellectual level.

(4) Exercise utmost discretion and avoid controversial discussions.

(5) Secure all names of other individuals who may have knowledge of the same information.

(6) Remember security regulations and make no commitments which cannot be fulfilled.

4—14. Interviewing a Witness

a. General. The nature of the information from a witness dictates the need for special consideration in the manner of interview. The importance of a witness is that he can provide direct evidence. A witness may also provide data and leads which, although they may not be usable in a legal proceeding, may serve to aid further investigation. In many respects, the general principles observed in interviewing voluntary sources are also applicable in interviewing witnesses; however, there are a few additional factors which have a bearing on the questioning technique.

b. Basic Psychology. The reputation, social standing, and profession of the witness, plus the fact that his statements are generally recorded for possible use in court, cause understandable psychological reactions. A normal person may be unable to prevent personal prejudice from causing distortion of his thinking and presentation of the facts, and a less conscientious person may not even attempt to be objective. The witness may not be aware that he is capable of distorting facts unwittingly, or that forgotten details might be replaced with the product of his imagination. The misgivings of a conscientious witness, who must make incriminating statements against another person, are understandable. The longer the lapse between the incident and the interview, the greater the possibilities that imagination may alter the facts. These psychological effects occasionally reveal themselves in the form of a witness' resistance to questioning and his refusal to testify. It may become necessary to apply interrogation techniques to witnesses who are unwilling to respond to questions asked during the interview (para 4—16 through 4—18). The witness may feel that once his testimony becomes public knowledge and he is identified, his personal affairs may be affected adversely. In some instances, the witness may visualize with misgivings a courtroom scene in which he will be the butt of a sarcastic lawyer's barbs and public ridi-
c. Circumstances or Conditions Affecting Questioning Witnesses. There are certain circumstances and conditions which may be present and which may affect the evaluation of the information received from a witness.

(1) The physical and mental qualifications and condition of a witness are the most accurate gauge of his value. The accuracy of the witness' observations may be affected; for example, if a witness stated that he observed something at a distance of 100 yards, the condition of his eyes would have to be considered in evaluating his testimony.

(2) Witnesses must have the capacity to observe, comprehend, and report. The qualifications of a scientist, for example, to testify on scientific matters within his field of interest would differ considerably from those of a layman.

(3) Categorical statements regarding the sex of a witness as a basis for evaluation are misleading. A woman's emotional traits may differ from those of a man, but instability is a characteristic not peculiar to either sex. These facts notwithstanding, the Special Agent must not ignore the fact that some women frequently rely upon intuition rather than critical analysis.

(4) A categorical statement with respect to age as a qualification for the competence of a witness also is not justified. Once a child has attained the age of reason, his testimony may be just as valid as that of a mature person. There are psychological patterns which fit certain age groups. The likelihood that children will falsify the facts in a deliberate attempt to influence the situation is relatively slight; on the other hand, their vivid imaginations are not hampered by the demands of logic and they tend to exaggerate.

d. Special Cases. The Special Agent's task is further complicated because he may deal with witnesses whose attitudes require a change in technique. The following are types of cases which require special treatment.

(1) There are witnesses who are indifferent to the problems of the Special Agent. Others flatly refuse to talk because of possible danger to themselves. The Special Agent should attempt to stimulate their cooperation by appealing to their patriotism, by pointing out that it is to their personal interest to talk, or by leading them into a logical path of reasoning.

(2) Some witnesses are eager to demonstrate their knowledge and to prove to themselves that they are indispensable members of society. They may be braggarts; they may talk too much; they may know it all. The Special Agent must be patient, weigh critically everything that is said, separate truth from fiction by asking pertinent questions, and analyze the information carefully by comparing with other known facts.

(3) Some witnesses are timid and others may be suffering from emotional stress and nervous tension. The Special Agent must attempt to quiet their fears by being patient and understanding. There may be occasions when the Special Agent will gain much by asking questions when the witness is extremely vocal due to his emotional condition; however, after the witness has calmed down, he should be questioned. Experience indicates that some witnesses offer the most factual information during periods of emotional upset because their normal mental processes, which would have permitted them to rationalize events and color their stories, are not functioning.

(4) A habitual liar obviously is a poor type of witness, but there are occasions when such a person is the only possible source of direct evidence against a suspect. In such an instance, the Special Agent cannot ignore the witness because of his weakness. Habitual liars usually contradict themselves; if the witness can be made to repeat his story often enough, the truth may emerge.

(5) A drunk witness should be questioned on the spot if possible. At the risk of being led through a conversational maze, the Special Agent should talk with the witness and strive to extract, by use of flattery, boastful disclosures which the witness might not make if sober. Later, these statements may be used as a basis for a formal interview or interrogation of the witness.

e. Method of Interview. (1) The Special Agent should, as soon as possible, but preferably prior to the interview, check his unit files for information about the witness. He also should be thoroughly familiar with all available facts of the case.

(2) The approach must include an attempt to anticipate and overcome the witness' objections, if any, to talking. As with a volunteer source, the witness should be put at ease.

(3) The witness should be encouraged to tell his story in his own way.
4—15. Evaluating a Potential Witness

The judge, jury, or other factfinding body will judge the credibility of a witness according to his persuasive effect. The probable persuasive effect of a potential witness can be assessed in advance of his appearance before the factfinding body by consideration of several factors:

a. **Capacity for Observation, Recollection, and Narration.** The witness who perceives all the details of what he observes and is able to recall these details and communicate the circumstances to a listener will have a very persuasive effect on any factfinding body. The degree to which these capacities have been developed can be tested in any number of ways to assist in the evaluation of a potential witness in advance of his appearance before a factfinding body.

b. **Appearance.** The physical appearance of an individual who may be used as a witness will have a decided influence on his persuasive effect. If he appears immature or his countenance constantly reflects doubt or lack of comprehension, he is not likely to appear highly credible to the jury or other factfinding body.

c. **Prejudice.** If a witness holds some prejudice which may influence or color his testimony, this should be considered in advance of his use as a witness.

d. **Agency Checks.** In some cases, it will be necessary to have local and/or national agency checks conducted on potential witnesses in an attempt to determine their reliability.

Section IV. INTERROGATIONS

4—16. General

Interrogation is the formal and systematic questioning of an individual in order to extract the maximum amount of usable information. The principles and techniques of interrogation contained in FM 30-15 are applicable to counterintelligence interrogations. Brief discussions of those aspects of interrogation peculiar to counterintelligence investigations are included here. Combat counterintelligence interrogations are described in chapter 12.

4—17. Interrogation of Suspects

   a. **General.** A suspect is a person believed to be associated with a prohibited activity. Prohibited activity includes not only the major crimes listed in AR 381-130 as the basis for complaint type investigations, but also violations of security regulations. A person may be suspected of being directly implicated in an overt act which threatens the security of the US Army or a command, or he may be suspected of sympathetic association with members of subversive organizations. In combat for example, the Special Agent may have little more to work with than scraps of information and his knowledge of the situation and area. Regardless of whether the suspicion is founded upon a minimum of information such as an unlikely story or unusual nervousness of a subject, or whether it is founded on a wealth of factual data, the Special Agent’s duty is to be objective and impartial in his search for facts. Paragraph 4—12 also concerns suspects when they are subjects of complaint-type investigations.
b. Psychological Aspects. The instinct of self-preservation is stimulated in an individual when he knows he is considered a suspect. This deep-rooted reaction frequently is reflected in stubborn resistance to interrogation. It is natural for the subject to consider the interrogation as a battle of wits in which he has much to lose and to look upon the interrogating Special Agent as the prosecutor. This attitude may prevail whether the individual is a guilty man fully aware of his crime or an innocent person fighting to clear himself of circumstantial evidence.

c. Purpose of the Interrogation. Special Agents must keep in mind the twofold objective of interrogations—detection and prevention of activity which threatens the security of the US Army and the collection of information of intelligence interest. Generally, in interrogation of a suspect, the Special Agent seeks a confession because it tends to expedite the flow of intelligence information the suspect possesses.

d. Preparation.

(1) Study of the case. The Special Agent must gather and digest all available material concerning the suspect and the case.

(2) Legal requirements. The Special Agent must be familiar with those legal principles and procedures (chap 3) which may be applicable to the case at hand. Legal requirements may differ, depending on whether—

(a) The US is at war or in a military occupation;
(b) The counterintelligence unit is operating in overseas areas;
(c) Status-of-forces or other agreements are in effect;
(d) The suspect is or is not a US citizen;
(e) The suspect is a member of the US Armed Forces; or
(f) The individual is a prisoner of war.

In case of doubt as to the legalities in the interrogation or the investigation, the Special Agent must seek clarification from higher authority, and with the cognizance of his superiors should seek the assistance of an appropriate judge advocate.

(3) Apprehension of suspect. Counterintelligence personnel have been given the authority to apprehend certain categories of suspects as outlined in AR 381–108. Normally, however, suspects are apprehended by other US and/or Allied agencies and referred to the CI element for interrogation because they are presumed to have information of counterintelligence interest. When counterintelligence personnel apprehend the suspect, the apprehension, search, and seizure of evidence should be performed in accordance with the principles and procedures given in FM 19–5. Basic rules of preservation of evidence, receipting and accounting for the suspect’s property, and maintaining the chain of custody of evidence must be observed (para 4–31 through 4–35). If the suspect is a military female, the Special Agent must advise her that she has the right to request a WAC of nurse officer (or any WAC or any female) to be present during the interview. If she waives this right, a female witness must still be within listening distance during the interview (either inside or outside the interview room) as provided in paragraph 16, AR 600–3. This additional female may be of assistance by conducting a body search of suspect when such a search is necessary. If the female is not in the military service, no requirement exists for either a female or a male to be present during the interview; however, paragraph 3–21c(8) AR 195–10 states that a witness should be within listening distance or present when a nonmilitary female is interviewed. In addition, a signed waiver should be obtained from the suspect or accused attesting to the waiver (para 4–12e(8)).

(4) A suspect not in custody. When the suspect to be questioned or interrogated is not in custody, preparations may include a consideration of a discreet approach (i.e., the suspect would be approached with some plausible reason as a ruse and questioned). Frequently there may be insufficient evidence to bring about the apprehension of a suspect, or operational considerations may dictate the advisability of not apprehending the suspect.

(5) Physical preparations. The Special Agent must insure the following preparations prior to an interrogation:

(a) The interrogation room must be available and free of distractions.
(b) If use of recording equipment is anticipated, it must be installed and checked for operating condition.
(c) If more than one Special Agent is to take part in the interrogation, the team must be thoroughly oriented on the case and the plan of interrogation.
(d) If witnesses or other persons are to be used to confront the suspect, availability of these persons must be arranged.
(e) Arrangements must be made to minimize unplanned interruptions.
Arrangements must be made for the suspect to be held in custody or provided billeting accommodations, if appropriate.

e. The Interrogation Proper. The basic techniques and procedures of interrogation given in FM 30-15 will be applied, as appropriate. The following points are particularly important in interrogations of suspects:

1. Use background questioning to provide an opportunity to study the suspect face to face.

2. Avoid misinterpretation and impulsive conclusions. The fact that the subject is a suspect may in itself create reactions of nervousness and emotion.

3. Do not permit notetaking to interfere with observation of the suspect's reactions.

4. Seek all details concerning the suspect's implication in prohibited activity.

5. Concentrate on the details of the story to detect flaws. Each statement of the suspect must be examined for its plausibility, relationship to other statements made or to facts known, and factual completeness. Discrepancies called to the suspect's attention which require adjustment frequently weaken the suspect's position.

6. Every cover story has a weakness; finding it is frequently the key to a successful interrogation.

7. Treatment required by Geneva Conventions must be strictly followed, as applicable.

f. The Confession. If the suspect desires to make a confession, a sworn statement, if possible, will be obtained and the procedures of chapter 3 will apply. As long as the suspect has been given an explanation of rights, any unsworn statement normally can be used in court against him. If the suspect is neither a citizen nor a member of the Armed Forces, requirements will be stipulated in the unit's SOP.

4-18. The Polygraph

The polygraph is frequently used as an aid to counterintelligence interrogations. The operation of the polygraph and its general application are discussed in FM 30-15. The conditions under which polygraph examinations are conducted within the Department of the Army are set forth in AR 195-6. Chapter 5 of this manual covers the application of the polygraph in counterintelligence investigations.

Section V. ELICITATION

4-19. General

Elicitation is a technique whereby information of value is obtained through a process of directed communication in which one or more of the parties involved is unaware of the specific purpose of the conversation. Elicitation is a planned and systematic process requiring careful preparation.

4-20. Preparation

Elicitation is always applied with a specific purpose in mind. The objective, or information desired, is the primary factor in determining the subject, elicitor, and setting for the elicitation effort. Once the subject has been selected, based upon his access to, or knowledge of, the desired information, there are numerous areas of social and official intercourse which may be exploited for the setting. Prior to the approach, all available intelligence files and records, personality dossiers, and knowledge of other individuals who have dealt with the subject in the past should be utilized in order to ascertain the individual's background, motivations, emotions, and psychological nature.

4-21. Approach

The subject should be approached in normal surroundings in order to avoid suspicion. There are two basic elicitation approaches, flattery and provocation. Many possible variations to these approaches may be used:

a. By appealing to the ego, the self-esteem, or the prominence of the subject, it may be possible to guide him into a conversation on the area-of-interest.

b. By insinuating that the subject is an author-
ity on a particular topic, his opinions may be solicited.

c. By adopting an unbelieving attitude, it may be possible to induce the subject to expound on the correct view or to answer out of irritation. Exercise caution so as not to provoke the subject to the point that rapport is broken.

d. By inserting bits of factual information on a particular topic, it may be possible to induce the subject to confirm and further expound on the topic. This approach does not lend itself to spontaneity.

e. By offering sincere and valid assistance to the subject, it may be possible to determine his specific area-of-interest.

f. By exhibiting an area of mutual or common interest, the subject may talk freely on the matter. (The elicitor must have more than superficial knowledge of the subject matter.)

4–22. The Conversation

a. Once the approach has successfully opened the conversation, techniques must be employed to channel and direct the conversation about the area-of-interest. Some common techniques include:

(1) Attempt to obtain more information by a vague, incomplete, or too generalized response.

(2) Elicit additional information in areas in which the subject’s response is unclear (i.e., “I agree; however, what did you mean by...?”).

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

b. To be successful, the elicitor must be resourceful; use initiative and imagination; and be unusually perceptive. He must be persistent without being obnoxious, and remain in complete control of the conversation at all times.

Section VI. SURVEILLANCE

4–23. General

Surveillance is a form of investigation which consists of keeping a person, place, or other target under physical or technical observation in order to obtain evidence or information pertinent to an investigation. It is a method which should be employed only when simpler and more economic procedures are not conducive to success. This method can produce accurate direct information but usually requires a considerable amount of planning, preparation, and extensive expenditure of manhours by trained personnel. It is used to amplify known data, confirm or refute allegations, obtain leads upon which to base further investigation, or provide protection.

d. To confirm or refute information furnished by informants or anonymous reports.

e. To obtain admissible legal evidence for use in court.

f. To obtain “probable cause” for searches.

g. To locate deaddrops, meeting sites and postal boxes.

h. To check on the reliability of informants.

i. To prevent the commission of espionage or sabotage.

j. To provide background for undercover assignments.

4–24. Objectives

Surveillance is often employed by investigators as an aid in achieving investigative objectives which vary with the requirements of the case. The most common objectives of a surveillance are the following:

a. To learn the identity of persons involved in a given activity.

b. To obtain information for a subsequent interrogation.

c. To develop leads for further investigation.

d. To confirm or refute information furnished by informants or anonymous reports.

e. To obtain admissible legal evidence for use in court.

f. To obtain “probable cause” for searches.

g. To locate deaddrops, meeting sites and postal boxes.

h. To check on the reliability of informants.

i. To prevent the commission of espionage or sabotage.

j. To provide background for undercover assignments.

4–25. Types of Surveillance

In counterintelligence operations, surveillances are commonly referred to by certain terms to indicate the relative intensity and sensitivity as well as the methods of execution. Inasmuch as a surveillance frequently includes a change of intensity or the simultaneous application of more than one method, it is inadvisable to treat these terms as inflexible categories.

a. Category as to Intensity or Sensitivity.

(1) Discreet. A discreet surveillance is one in which every effort is made to insure that the
subject remains unaware that he is under observation. Although every effort is made to gain as much information as possible, the paramount consideration is that the subject not become aware of the surveillance. Generally, the guiding rule is to discontinue surveillance rather than risk actions which make the subject aware of the surveillance.

(2) Close. A close surveillance is one in which maintaining constant observation of the subject is the paramount objective, even though he may become aware of the surveillance. Surveillance to provide protection is frequently of this nature inasmuch as the subject is generally the person to be protected.

b. Category as to Method.

(1) Fixed. A fixed surveillance is one in which the surveillant(s) remains in a relatively fixed position to observe the activities at a specific location.

(2) Moving. In a moving surveillance, the surveillant(s) follows the subject from place-to-place to maintain continuous watch over his activities. The movement may be by foot, or by vehicle, to include land, water and air, or any combination of these.

(3) Technical. Technical surveillance is accomplished by the use of technical visual devices, electronic equipment, and photography. Chapter 5 and the classified supplement to this manual, FM 30-17A, discuss techniques and procedures employed for this and other investigative purposes.

(4) Combination or Mixed. A combination of technical, fixed and moving surveillances are usually the most expensive in terms of money and personnel but will usually achieve the best results. Two of the most common are the progressive and checkpoint surveillance.

4-26. Preparation for Surveillance

Regardless of the purpose, sensitivity, or method of a surveillance, the degree of success or amount of information obtained is generally proportionate to the thoroughness of advance planning and preparation. Although short advance notice of the requirement for a surveillance is sometimes necessitated by the sensitivity or criticality of the information to be obtained, the following planning and preparatory measures should be taken to the extent time permits.

a. Area and Target Study. All available information on the area in which a surveillance is to take place should be studied and analyzed. The areas in which the subject lives, works, and spends leisure time must be considered. If possible a reconnaissance should be made of the road, transportation, and traffic systems in areas in which a moving surveillance is anticipated. The nature, location, and types of buildings likely to be encountered during a surveillance should be considered. Study of the subject should include physical description, manner of dress (with emphasis on peculiarities contributing to ready identification under various conditions, particularly from the rear), habits, interests, probable degree of suspicion that he might be under surveillance, type of transportation generally used, names and addresses of likely contacts, financial status, walking gait, and other factors which will aid in pinpointing problems to be encountered by the surveillants. More extensive preparations, including such things as renting a room or an office in the area, studying the physical characteristics of the building, procuring technical equipment for observation and communication, and establishing a cover or plausible reason for being in the area will be required if the fixed surveillance is to continue over an extended period of time.

b. Surveillance Plan. Once surveillance has been directed and the area and target have been studied, a plan for execution should be developed. The plan must establish the number and type of personnel required, the general and specific instructions for the surveillants to insure that the overall objective of the surveillance is understood, and the operational limitations or special instructions which may have been imposed. The plan must assign specific tasks to teams or individual surveillants, provide for administrative and logistical support, prescribe communication methods and procedures, and establish necessary control measures. The degree of complexity of the operation and the time available will determine whether the plan is formal or informal, oral or written. The plan should be sufficiently detailed to prevent misunderstanding and confusion, but it should not be so restrictive as to eliminate all flexibility or to preclude the exercise of all initiative by individual surveillants. Every possible contingency should be visualized in planning and preparing for a surveillance; however, mobile surveillants, in particular, must not be overburdened with special equipment.

c. Selection of Personnel. Selection of personnel to participate in a surveillance must be done
with care, as an unqualified person can readily compromise the task and perhaps make other facets of the investigation even more difficult. If a choice must be made between conducting a surveillance with an inadequate number of qualified surveillants and a full complement which includes several unqualified personnel, the former choice is preferable. The principal qualifications of surveillants include:

(1) An inconspicuous appearance. An otherwise qualified person must be disqualified from participation if he has some outstanding physical feature or possesses mannerisms which will draw attention to his person.

(2) Ability to remain unnoticed. The surveillant must be able to blend with his surroundings in a wide variety of environmental conditions. Thorough area and target study contribute to the surveillant's success in adapting himself to varying circumstances without attracting attention to himself.

(3) Resourcefulness. The surveillant must be able to meet unexpected situations with poise and presence of mind. Resourcefulness is especially valuable when it is necessary to locate a subject who has eluded or otherwise become lost to the surveillant(s).

(4) Patience and physical stamina. Nearly every surveillance will include long periods of relative inactivity during which the surveillant must remain alert and prepared for an eventual-ity.

(5) Keen sensory perception and retention memory. The surveillant must develop the ability to examine systematically what he sees or hears so that details will register clearly in his mind. Opportunities for making notes may be limited, and a good memory for details is a very valuable attribute.

(6) Prior surveillance experience. It is essential that a maximum number of participating personnel have previous experience in surveillance. The details and techniques required, particularly for team operations, cannot be learned completely from textbooks or by participating in a few exercises. Experience must be gained in simple surveillance of less sensitive subjects and in protective surveillance operations of a more routine nature. A CI unit in an area where surveillance can be anticipated should maintain one or more surveillance teams of Special Agents. The success of a team surveillance is frequently dependent on the experience gained through working together. Practice surveillances serve to perfect the coordination of team members.

d. Personnel Limitations.

(1) In overseas areas, it frequently will be necessary to use indigenous personnel as surveillants since US personnel in some areas or locales would be conspicuous. These natives should have the appropriate physical characteristics, customs, dialects, economic status, and other characteristics necessary in the area concerned.

(2) When indigenous personnel are used, US personnel should be used as the control and supervisory element of the surveillance team, as well as for other broad aspects of the surveillance effort. These indigenous personnel should also be full-time employees of the MI unit. This will insure, as fully as possible, their loyalty to the unit. Their association with the unit must not be well-known to avoid compromise and should not be normally used in surveillances involving American personnel.

(3) The US surveillance team commander should participate in the surveillance for control purposes but he should stay in the background. The team commander should be familiar with the language, racial characteristics, and other social aspects of the area. He must train the indigenous surveillants in his general method of operation.

e. Administrative and Logistical Arrangements. These arrangements will require advance planning and preparation to support a surveillance. They include, but are not limited to, the following:

(1) Relief from other duties and issuance of appropriate orders, when required, for surveillance personnel.

(2) Procurement of any special documentation which may be required.

(3) Provision of funds to cover projected and contingency expenditure.

(4) Arrangements for transportation for moving surveillance as well as transportation to and from fixed observation points.

(5) Special supplies, such as special clothing, photographic equipment, audio and communications equipment, and similar logistical items.

(6) Arrangements for the surveillants to eat, if it would be unwise for them to enter restaurants, or if they cannot get to an eating establishment.
(7) Issuance of firearms if necessary or required.

(8) Preparation of a cover story to explain the surveillants’ presence and activity in given areas (ditch diggers, surveyor, traffic counters, etc.).

(9) Details on shift changes planned well in advance.

f. Communications and Control Arrangements. The success of a surveillance is frequently dependent upon a reliable means of communication between the control element and the surveillants. Radio, telephone, sound, or visual signals may be employed alone or in combination. Aerial and visual signals to be used between the surveillants must be developed carefully to allow flexibility and preclude compromise and must be practiced to insure recognition during an actual surveillance. When possible, radio communication should be established as the primary means of communication between operating elements and the surveillance control point. Under certain conditions, consideration should be given to the use of secure communications systems such as operational codes and voice security equipment. Regardless of the communication arrangements, it is essential that one central point be established for direction and control of operations at all times. The chain of command must be clearly prescribed from the individual surveillant to the control point.

4–27. Conduct of Surveillance

a. Fixed Surveillance. A fixed or stationary surveillance may vary from intermittent periods of short observation to a carefully prepared observation point operated on a 24-hour basis over an extended period. It may be conducted from an outside standing post, a vehicle, or within a building. It often includes the use of photographic equipment, and frequently a technical surveillance is also involved. Surveillance from a fixed observation point is physically and mentally exhausting. If the observation is to continue over too long a period, arrangements for frequent relief should include provisions which will allow the relief surveillance personnel to arrive and the relieved personnel to depart without attracting such notice as might compromise the surveillance. If a fixed vehicular surveillance is used in a neighborhood at night, the car doors should be opened and closed since people unconsciously listen for car doors to close after hearing a car stop.

b. Moving Surveillance.

(1) Foot surveillance. When a foot surveillance is employed, it is essential that it be conducted by a team rather than by an individual surveillant. There may be a few occasions when a foot surveillance has to be conducted with only one surveillant, but these are exceptions. The general inadequacy of results obtained and the greater risk of compromise militate against the use of a lone surveillant who normally will conduct a fairly close surveillance.

(a) ABC method. The most common procedure for the foot surveillance is referred to as the “ABC” method (fig 4–1). One member of the team takes a position (A) a short distance (distance will depend on the environment, number of people in the area, and nature of the area) behind the subject(s). Another takes a position (B) behind A, and a third takes a position (C) on the subject’s flank, usually across the street. If the team has other members, they follow behind B and C. Such a surveillance over an extended period of time may require replacement to prevent the subject from recognizing a surveillant. It is best to relieve the surveillance team one at a time at staggered intervals to insure continuity and avoid confusion. Prearranged visual and/or audio signals are usually essential to the success of a foot surveillance.

(b) AB method. A less desirable but acceptable technique for a foot surveillance is referred to as the “AB” technique where the surveillant directly behind the subject is again in the A position. The B position can either be behind A or on the subject’s flank. When both surveillants operate on the same side of the street as the subject, and the subject turns a corner, A continues in the original direction and crosses the intersecting street. From his vantage point across the street, A will then signal the correct procedure for B to follow. B should not turn the corner or come into sight until he has received the signal. When B is operating across the street and the subject turns a corner to the right, away from B, B will cross the street behind the subject and take up the A position. This move should be prearranged, and no signals should be necessary. All visual signals employed should be discreet and consistent with the environment (fig 4–2). If the subject turns to the left and crosses the street toward B, B should drop back to avoid meeting the subject. B could go into a store or continue straight ahead. B should keep A in sight to observe his signals indicating what the next move should be.
Figure 4-1. "ABC" method of surveillance.
Figure 4-2. "AB" method of surveillance.
(c) One-man method. A one-man surveillance should be avoided in a moving surveillance because it does not provide for flexibility. Its best employment is in a fixed surveillance. If a moving one-man surveillance must be resorted to then the surveillant should operate to the rear of the subject when on the same side of the street, and keep as close to the subject as possible to observe his actions. Crowd and street conditions normally dictate the appropriate distance to be maintained between the subject and the surveillant, however, consideration must be given to the prevailing light conditions, the subject's evasive actions, and the Special Agent's personal desires. As a general rule, the more people on the street, the closer the surveillant stays to the subject. If the subject turns a corner in an uncrowded area the surveillant should continue across the intersecting street. By glancing up the street in the direction the subject traveled he can note the subject's position and actions, and act accordingly. The surveillant can then operate across the street from the subject, recrossing the street at his leisure to fall back in behind the subject. When the subject turns a corner on a crowded street, the surveillant should stop at the corner and unobtrusively observe the subject's actions. Unless the subject is standing just around the corner, the surveillance can be continued from the same side of the street. Whatever the conditions, however, the investigator should not turn a corner immediately behind the subject. When operating from across the street, circumstances will dictate whether to operate forward, to the rear, or abreast of the subject. It is best if the surveillant can be abreast of the subject when he turns a corner to enable the observation of any contact made or an entry into a building.

(2) Vehicular surveillance. Under most conditions, two or more vehicles are required to conduct a vehicular surveillance, although, traffic conditions permitting, one may suffice for a short period of time. The first car should remain some distance behind the subject with not more than one or two vehicles between it and the subject's vehicle if the traffic is at all heavy. The second car should be further behind or following a parallel route one or two blocks away (fig 4-1, 4-2). At times, one car may precede the subject; in any event, the surveillance cars should alternate positions frequently to reduce the chances of subject's recognition of the surveillance cars. These "profiles" can be changed by shifting occupants (front-to-rear or rear-to-front), adding or dropping an occupant, changing license plates, placing packages on the rear window ledge or removing them from the ledge, or similar changes. In addition, frequent changes of cars must be considered. Radio communication between surveillance cars is normally available (FM 30–17A). If radios are not available, a set of visual signals must be arranged to coordinate the movement of the cars. Care must be exercised to prevent use of the radio equipment from attracting undue attention. When the driver is the only surveillant in the car, it may be useful to place a small tape recorder in the car with him which he can use for his notes instead of a distracting pad and pencil. Advance coordination of a vehicular surveillance with other agencies, particularly the police, is desirable and essential in some areas. The police need be informed only to a degree commensurate with security of the activity. To aid in identifying subject's vehicle under adverse traffic, weather, or light conditions, it may be possible to equip the subject's vehicle with some recognition device which the subject will not notice. For example, reflective tape could be placed on the vehicle's undercarriage, or one taillight could be replaced with one of higher intensity. Under certain conditions, it may be possible to use surveillance vehicles with direction-finding radio equipment, e.g., attaching a small transmitter to the subject's vehicle and thereby following or locating his vehicle by the transmitted signal. Vehicular surveillance must be practiced to achieve any degree of professionalism. The driver must gain experience so that he depends mainly on the other occupants of his car for observation, thus devoting his attention to the driving. Again, the ABC method is highly preferred, but in cases where only two vehicles can be employed, both vehicles should follow the subject at different distances on the same street, (fig 4–2) as in the AB method of foot surveillance. This technique can be varied by having one vehicle going in the same direction as the subject on a parallel street while receiving radio-transmitted directions from the surveillants directly behind the subject. This technique is more flexible than the one-vehicle surveillance in that two vehicles can exchange places from time-to-time, or one vehicle can precede the subject. If more vehicles and people are available, other techniques can be planned that are even more flexible. When one vehicle is used for surveillance it must remain far enough behind to escape detection. When the subject's vehicle turns a corner, the surveillants may continue to follow, or they may make one of two possible moves to help break up the following pattern (fig
4–3). They may continue in the original direction, cross the intersecting street and make a U-turn; the subject will take little interest in a vehicle turning into a street behind him coming from a direction that is opposite to that which he was traveling before turning the corner. An alternate move would be to continue in the original direction, crossing the intersecting street and continuing around the block. The subject will not expect to be under surveillance by a vehicle approaching him from a frontal direction.

c. Mixed or Checkpoint Surveillance. When the daily pattern of activity of a subject under investigation is relatively constant, a checkpoint surveillance can be employed. It consists of placing mobile, fixed, or technical surveillants at strategic points to mark the subject's progress from one point to another along routes normally used by the subject. Foot or vehicular surveillants, depending on subject's mode of transportation, can be placed to the rear and/or front of the subject but at a greater distance than is normally used in

Figure 4–3. One-vehicle surveillance.
a discreet surveillance. When the subject deviates from his normal pattern, these floating surveillants would then proceed into a normal discreet surveillance. Many variations of this technique can be used.

d. Progressive Surveillance. Progressive surveillance is employed in cases when the experience and caution of an important subject make extreme care mandatory. Whether or not he notices any evidence that he is being followed and because of the importance of his mission, the subject will resort to every technique and subterfuge to elude possible surveillance. By following the subject only a short distance each day, the surveillant minimizes the probability of detection by the subject. This type of subject will be most cautious when emerging from his home or office, and for the first several blocks, or comparable distance, will take measures to elude surveillance. After subject’s residence, office, or other starting point has been located, the surveillants, generally by trial and error from day-to-day, pick up the subject some distance from the starting point and follow or observe him only a short distance on the first day. On the second day, the surveillants endeavor to pick up the subject at the time and place they left off the day before, and then follow or observe him a short distance to a new point. If the subject varies his daily routine once in a while, this method will be painfully slow, but it will eventually lead the surveillants to those contacts which the subject is trying to keep secret.

4-28. Surveillance Techniques

Although no predetermined solution can be established for all situations encountered during surveillance, there are several general guidelines which will aid in determining action to be taken in situations which are commonly encountered.

a. Identification. The subject should be pointed out to all members of a surveillance team, although in some cases a picture or detailed description must suffice for identification purposes. Each surveillant must study the subject’s physical appearance and mannerisms so that identification under all conditions will be facilitated. Do not rely on subject’s dress for identification.

b. Remaining Inconspicuous. The surveillant must be constantly aware of his surroundings to be able to proceed with an apparently natural and deliberate act if the subject should approach him directly or evince undue interest in his actions. Entering a business establishment, asking directions of a passer-by, or merely pausing to light a cigarette are examples of natural actions which may allay the suspicions of the subject. Minor changes in dress to present a new pattern of appearance also contribute to maintaining an inconspicuous appearance. Such things as putting a rolled up newspaper in a topcoat pocket, changing from a necktie to a bowtie, wearing or removing a hat or spectacles require little time and are very effective in altering an appearance outline of the individual.

c. Encountering Acquaintances. During a surveillance over an extended period of time, a surveillant may encounter acquaintances or even members of his own family while he is engaged in following the subject. The general rule in such cases is to avoid recognition and ignore the presence of the acquaintance or relative if at all possible. If this cannot be done the surveillant must be prepared with some acceptable excuses for limiting the encounter to a brief natural exchange which will permit him to continue the surveillance without interference. Encounters of this nature are to be expected and prior plans must be made through prearranged signals to those assisting for any changes that may be required.

d. Eye Contact. Normally the surveillant should avoid any direct eye contact with the subject, since the impression made on his subconscious mind may be manifested in later recognition and consequent suspicion. However, a hasty deliberate move to turn aside when confronting the subject is an unnatural and obvious action, which may make a deeper impression than direct eye contact.

e. Using Conveyances.

(1) Taxicab. If the subject enters a taxi, the surveillant should attempt to obtain another cab or vehicle in which to follow. In a large metropolitan area, it is possible that any taxi driver will accept instructions to follow another car without question or evidence of special interest, particularly if his efforts are rewarded with a more substantial tip. However, the surveillant should be prepared in all cases to provide the driver with some innocuous but logical explanation if the driver is reluctant to comply with the request. If necessary, the presentation of credentials or badge for this purpose may be effective, but this procedure will be governed by prior instructions from the unit controlling the surveillance. If the surveillant is unable to obtain any
vehicle to follow subject's taxi, he should note the name of the cab company, the cab number, license tag number, and the time and place of loading. This information should be relayed to the surveillance control point as soon as possible, to determine, if required, subject's route and destination through the appropriate cab company and/or authorities.

(2) **Bus or streetcar.** The surveillant should try to enter the same conveyance as the subject and position himself to the rear of the vehicle and behind the subject. If he misses the bus or streetcar, he may be able to use a taxicab or other means to overtake and board the bus or streetcar at a subsequent stop.

(3) **Plane, bus, or railroad.** If the subject enters a station or terminal and purchases a ticket, the surveillant should discreetly attempt to obtain as much information as possible regarding the trip. A position in line one place removed from the subject will often afford the opportunity to overhear the discussion between the subject and the clerk without any indication of obvious interest. The limits imposed on the surveillance will govern whether or not the surveillant purchases a ticket and follows subject on his trip. In many cases, an air shuttle will arrive sooner than a scheduled airline and can be used in getting to the destination ahead of the subject for resumption of the surveillance or for boarding the same aircraft with subject. The ease of boarding air shuttles will alleviate certain surveillance requirements. If the surveillant is not to follow subject, he should attempt to obtain as much of the following data as possible so that the surveillance may be resumed by another counterintelligence unit either en route to or at subjects' destination:

(a) Description of subject's dress, emphasizing outstanding items which might facilitate recognition.

(b) Description of hand baggage and hold baggage.

(c) Date and time of departure and date, time, and place of arrival at destination.

(d) Name and number of the train, plane flight, or bus and type of accommodations (coach, sleeper, first class, etc.).

(e) Any other details which will facilitate resumption of surveillance en route to or at destination.

*Entering Buildings.* The size, nature, and surrounding locale of buildings entered by subject are significant considerations in determining further action.

(1) **Small building.** If the building has exits which can be kept under observation from a discreet outside position, the surveillant normally should not enter. However, if the previous pattern of activity indicates that the subject may make a contact or engage in some other action pertinent to the investigation, the surveillant should enter by an entrance other than that used by the subject, or otherwise convey the impression that he has arrived at the building from a different direction than the subject.

(2) **Large building.** A surveillant normally will follow the subject into a large building such as a department store or office building. Within the building, the surveillant must take advantage of the building layout to observe subject without attracting attention to himself. Magazine and cigar counters in office building lobbies will often afford cover for the surveillant's actions immediately after he enters the building. If the subject enters an elevator, the surveillant should also enter if there are passengers and the subject is unsuspecting. The surveillant may ask for the floor below or above that requested by the subject. In the latter case, the surveillant should then use the stairs to reach the same floor as the subject in order to resume his observation. If the elevator is used and the surveillant gets off on the same floor as the suspect, the surveillant should immediately move to a particular counter or department on that floor. Loiterers are conspicuous. If the subject enters an elevator as an only passenger, the surveillant should remain in the lobby and determine subject's destination by watching the floor indicator. Surveillance can then be resumed by using either the stairs or the elevator to reach the same floor as the subject.

(3) **Hotel.** If the subject registers at a hotel, the surveillant should attempt to ascertain the room number by observation of the registration process from a discreet distance. Since the room keys are normally maintained on a numbered board or in boxes directly behind the clerk, it is usually possible to observe which key is withdrawn and given to the subject. The surveillant should exercise caution in seeking the assistance of hotel staff personnel to obtain a room adjacent to the subject, monitor his mail, obtain a record of incoming calls or telegrams, examine the register, or take any other action connected with the investigation. In overseas areas in particular, hotel staff personnel frequently have ties with the
telligence and subversive organizations. The unit SOP or policy on such matters must be known thoroughly by the surveillant.

(4) Motel. If the subject's vehicle enters a motor court, the surveillant should not follow immediately, but from a discreet distance he should attempt to observe if the subject registers and to which cabin or unit he proceeds. Should it then be determined advisable for the surveillant to also register, he must exercise caution. He has not only the problem of remaining inconspicuous himself but he must keep his vehicle from attracting subject's attention. Many motels are similar to hotels; in such instances, the same guidelines will apply.

(5) Restaurant. When the subject enters a restaurant, the surveillant must seat himself out of the direct view of the subject but with a view of the subject. If the subject is accompanied by others, and their conversation is deemed to be of probable interest to the investigation the surveillant should attempt to place himself within hearing distance. The surveillant must give attention to the type of service ordered by the subject and govern his own order accordingly to insure that he will be able to pay his check and depart from the restaurant without disrupting the surveillance when the subject leaves. In some instances, the departure of the subject can be anticipated, and it may be advantageous to pay the check and leave ahead of the subject, provided that this can be done without attracting the subject's attention.

(6) Telephone booth. When the subject enters a phone booth, the surveillant must consider the following possibilities of gaining information which may contribute to the investigation:

(a) It may be possible to use a adjoining booth to overhear the conversation of the subject.

(b) The subject may leave the phone book open to the page containing the name of the person called, or he may note the number on the phone booth wall or a slip of paper which can be retrieved by the surveillant.

(c) The surveillant may be able to ascertain the number called by observing the dialing action of the subject. If the number of coins deposited indicates that the call is long distance, the surveillant should note the exact time of the call and obtain the telephone number of the booth from which the call was placed to aid in an attempt to trace the call.

(d) The time spent in the phone booth by the subject will afford the surveillant an excellent opportunity to find a suitable point from which to make a photograph, if required, as the subject emerges from the booth.

g. Subject is Lost. If the subject is lost during the surveillance, the first action is to report this fact to the surveillance control point. Relocating the subject is most often accomplished by studying the pattern of his prior actions and establishing temporary fixed surveillance at points he is most likely to visit. If the loss-of-contact took place during a moving vehicular surveillance, it is often possible to resume observation by systematically searching the general area where subject disappeared, using lookouts at major intersections, and giving special attention to parking lots and sidestreets. Subject may also reappear in the area where he was last seen. Pretex calls to his home or office may also locate his whereabouts. The use of a square or box pattern in the area where the subject was last seen may also yield results if radio communications are available for reassembling the surveillance team should subject be located by a single surveillant. Assistance from police or other authorities should not be requested without approval from the surveillance control point.

h. Compromise of Surveillant. If the subject of a discreet surveillance clearly indicates by his actions that he has become aware of the surveillance, the surveillant should withdraw from the area, discontinue the surveillance, and notify the control point. The surveillant should insure that his departure from the area is conducted in an unobtrusive and natural manner, regardless of the degree of his certainty of compromise. The surveillant must always be prepared to offer a logical response if confronted by the subject and accused of following him. In such case, a good offense is often the best defense; a belligerent denial of the allegation, coupled with a threat to summon police, may succeed in deceiving the subject. If an incident or occurrence draws the subject's attention to one or more of the surveillance team members, those members must drop from the team and withdraw from the area. Possible recognition of a team member or members at a later date could be avoided by this action. Eye contact between a surveillant and the subject is usually sufficient cause for the surveillant to drop from the team.

4–29. Detecting Surveillance

It is important for the Special Agent to know various means of detecting surveillance so that he
will recognize such action when taken by the subject of a surveillance, but also so that he may employ these devices himself en route to covert meetings, cover locations, or other locations when he desires to insure himself against surveillance. Some of the most common and effective means of determining if a surveillance is in progress are—

a. Use of a "Convoy". A person who suspects he is under surveillance, or who anticipated surveillance, may employ the services of one or more colleagues to follow him at a distance to determine if he is being followed. The assistant is termed a "convoy" or countersurveillant. This means is one of the most effective in detecting surveillance.

b. Retracing Course. By changing direction of movement several times in a short span of time and retracing his course, a person who suspects surveillance may be able to determine if he is being followed. This procedure is equally effective for detecting foot or vehicular surveillance.

c. Window Reflections. In business districts, a subject concerned about a possible surveillance may pause in front of a large show window for the ostensible purpose of window shopping, and then observe the reflections of passers-by to spot indications of surveillance.

d. Use of Bait. The subject may throw away a scrap of paper, an envelope, or some similar item which would be of interest to anyone following him. He will then use window reflections or a similar means of observation to determine if anyone retrieves the bait.

e. Change of Pace. In areas where pedestrian and vehicular traffic is relatively sparse, the subject may detect surveillance by moving very slowly for a distance, then changing to a very rapid pace, and later again changing to a slow pace. The subject may couple this procedure with a sudden stop after turning a corner in order to observe the actions of those behind him. These procedures may be encountered in both a foot surveillance and a vehicular surveillance.

f. Actions on Public Conveyances. On conveyances, a person who suspects or anticipates surveillance may employ a variety of actions to test for the presence of surveillance.

(1) The subject may board the conveyance, pay the fare, and then get off just as the vehicle starts to move, observing the actions of others who have boarded at the same stop to see if anyone attempts to follow.

(2) The subject may leave the conveyance in an area with little pedestrian or vehicular traffic and then loiter in the area to determine if a suspected surveillant dismounts at the same stop, or the next one.

(3) The subject may board several successive conveyances along a single route within a short period of time and watch for faces which reappear.

g. Automobile Tactics. If the subject of surveillance is driving an automobile, he may use traffic signals and other controls to advantage to determine the presence of surveillance vehicles. For example, he may time his approach to a traffic light so that he will pass through the intersection just as the light turns to red and then watch the rearview mirror to determine if any other vehicle commits a deliberate traffic violation in order to follow him. He may also drive the wrong way on a one-way street, feign motor trouble in a sparsely traveled area, or employ a wide variety of other tactics to test for surveillance.

4–30. Eluding Surveillance

Many subjects who suspect surveillance, or because of the clandestine nature of their activities, expect it, will take steps to elude the observation. Common and effective measures for eluding surveillance include—

a. Entering and Leaving Crowded Buildings. In business areas, a person seeking to evade surveillance can usually succeed with little difficulty by hurrying in and out of crowded buildings and taking advantage of multiple entrances and exits found in larger buildings.

b. Concealment. The subject may elude his surveillance by dodging into an available entrance immediately upon rounding a corner and disappearing. Entry into apartment buildings for this purpose can usually be gained by pressing a number of bells to the various apartments. At least one person will usually respond and release the entry latch, after which the subject may enter, remain concealed, and later depart by using a rear entrance.

c. Use of Decoy. The subject may engage a substitute of like physical appearance to act as a decoy to mislead the surveillants. This technique can be employed most effectively when the decoy is put into service from the subject's place of residence or of employment, as surveillants are less
likely to doublecheck identification at such points.

d. Change of Appearance. The same tactic employed by a surveillant to avoid becoming conspicuous can be equally effective for the subject seeking to elude surveillance. Changing appearance is particularly effective where, because of crowds or limited visibility, the surveillants are forced to rely on color of clothing or silhouette to maintain contact.

e. Dodging. Pursuing an erratic course through dense pedestrian or vehicular traffic is effective, particularly when traffic controls are used to the maximum advantage.

Section VII. COLLECTION AND HANDLING OF PHYSICAL EVIDENCE

4–31. General

a. Physical evidence is tangible in nature and recognizable in form. It tends to prove or disprove a fact in dispute. It includes all articles and material collected in connection with an investigation to establish the identity of the perpetrator and the circumstances under which an incident occurred. These articles and material are used to aid in the prosecution of the offender or in other termination of the case. Physical evidence may be encountered in any type of counterintelligence operation, and its importance is not limited to those investigations likely to result in a court trial. Physical evidence of probative value is often essential to the proper determination of administrative action such as the granting of a security clearance, the issuance of a visa for entry into the United States, or the admission of an alien into the Armed Forces.

b. It is not expected that every Special Agent will be an expert in physical evidence. The analysis of various substances normally will require the services of one or more specialists such as ballistics experts, chemists, and fingerprint technicians, to fully identify the substance as contributing to or not contributing to the crime. However, the Special Agent should have a general knowledge of the value, limitations, and characteristics of physical evidence and should be able to recognize, collect, handle, and preserve evidence encountered during the course of investigation. The following publications will be of value for reference and training purposes: AR 190–22, FM 19–5, FM 19–20, Army Subject Schedule 19–29, and Technical Bulletins of the Provost Marshal General (PMG)-series. He should also be familiar with the procedures of his unit for obtaining the assistance of appropriate experts and laboratory facilities.

4–32. Documentary Evidence

Documents are the most common items of physical evidence encountered by counterintelligence personnel. Manuscripts, magnetic tapes, records, files, reports, sworn statements, photographs, video tape movies, pamphlets, maps, sketches, passports, identity papers, and similar documents are likely to be collected in counterintelligence operations.

a. Questioned Documents. Questioned documents are those whose validity is disputed. FM 19–20 describes various categories of questioned documents and types of assistance available from criminal investigation experts and laboratories. This assistance may be obtained through liaison with the appropriate provost marshal’s office.

b. Documents Containing Codes and Ciphers. Codes and ciphers (cryptography) are often used in communications between operational elements of espionage agencies. Unless the key to the system has been obtained, the investigator should not expend any time attempting to decrypt the message. The document, along with a history of the circumstances under which it was obtained and a brief summary of the related investigation, should be given to the nearest United States Army Security Agency (USASA) unit in accordance with FM 30–15.

c. Documents Suspected of Containing Secret Writing. Secret writing or the concealment from visible detection of written material by means of invisible inks, specially treated papers, microphotography, and similar systems, are also important facets of espionage communications systems. Documents taken from espionage suspects, or otherwise obtained under conditions indicating the possible presence of secret writing, should be tested for indications of secret writing. FM 30–18 and DIÄM 58–11 contain guidance on the handling of documents suspected of containing concealed writing. No attempt should be made to recover any secret text. The material should be forwarded to a facility or agency where the expertise is available.
4–33. Other Types of Evidence

Traces and clues often may be found in the form of latent fingerprints; firearms and ammunition; indentations made by tools, tires, or shoes; and from deposits of foreign substances such as fibers, soil, and stains.

a. Fingerprints. Fingerprints offer one positive means of identifying individuals since they never change throughout a person's lifetime. Surface fingerprints can be transferred, photographed, and developed by various techniques, thus providing invaluable evidence for purposes of identification. Detailed consideration of fingerprint patterns and methods of collection and preservation are included in FM 19–20. Assistance of fingerprint experts of the criminal investigation elements of the area provost marshal may be obtained through liaison.

b. Indentations and Fractures. Physical impressions and indentations left in various media are often of value as evidence; e.g., footprints, tool marks, and markings left on ammunition by the weapon from which it is fired.

(1) Tire imprints may identify a particular vehicle by association of the brand, amount of wear, and unique scars. Direction of travel can often be determined from the direction in which sand, soil, or water was thrown; the speed, from the distinctiveness of the track; and the weight of the load, from the depth of the track.

(2) Footprints may reveal direction and speed of movement, sex, approximate height and weight, and physical deformities. In addition, the brand of footwear may be apparent and provide additional leads.

(3) Firearms and bullets have individual characteristics which are subject to scientific examination for identification purposes. Each firearm and each bullet fired therefrom has individual characteristics which may be detected by expert examination under a microscope. The weapon will have on it the name of the manufacturer, a trademark, serial number, and possibly fingerprints or distinctive features. When discharged, a cartridge casing and bullet will have such characteristics as scratches or indentations associating them specifically with a particular weapon.

(4) Tool marks sometimes indicate the type of instrument used, since frequently impressions or abrasions will be apparent at the place of use. The presence of such marks may constitute important evidence in the investigation of security violations in which forced entry is apparent.

(5) Glass fractures, if examined by an expert, may reveal the direction of the blow or the type of instrument employed to break the glass. The nature of a projectile which pierced the glass can sometimes be identified. Since each type of glass has peculiar characteristics, examination may serve to identify the manufacturer of the glass and thus provide leads in some investigative situations.

(6) Serial numbers and trademarks are impressed by manufacturers on many items. Normally they are found on weapons, high-grade locks, watches, binoculars, precision instruments, power tools, and automobile engines. If the original number has been obliterated, a crime laboratory can often bring it out.

c. Fibers. Hairs and fibers have distinctive characteristics which may be useful in identification. They may be classified as animal, vegetable, mineral, and synthetic.

(1) Animal fibers include hair, wool, silk, and fur. Each type can be distinguished from another and many types have individual characteristics which permit further differentiation. By study of the diameter and texture of a human hair, for example, determination can sometimes be made of the race, sex, and general age of the individual.

(2) Vegetable fibers include cotton, linen, jute, and sisal, each of which has its own distinction such as color of dye and number of strands per thread.

(3) Mineral fibers include glass and asbestos.

(4) Synthetics have expanded much beyond the well-known rayon and nylon, but each can be distinguished from other types by laboratory analysis.

d. Soil and Stains. Samples of soil can provide information of value when examined microscopically and chemically. Study may indicate a difference between soil and dust, the latter being composed chiefly of vegetable fibers. Soil analysis may reveal the geological source or general origin, and at times a specific area of origin. Stains resulting from any cause are susceptible to analysis in a laboratory. They may be identified as food, vegetable matter, grease, oil, paint, rust, or body fluids.

e. Laundry Marks. Dry cleaning, laundry, and other clothing or linen marks, whether they be
made with indelible or invisible ink, may provide valuable clues in identification. Police usually maintain records which can help with this type of identification.

f. Detective Dyes. Police at times employ dyes and fluorescent powders which can be dusted or sprayed on items likely to be handled by suspects. Some of these are virtually indelible; others, invisible, but susceptible to detection under ultraviolet light for prolonged periods after contact.

4—34. Handling of Physical Evidence

a. All counterintelligence personnel should be familiar with the material on evidence or evidentiary property contained in FM 19–20. A guide to the procedures for handling physical evidence is outlined in figure 4–4. The Special Agent acquiring items of physical evidence is personally responsible for their safekeeping until he turns them over to the designated custodian of unit evidence. The custodian is, thereafter, responsible for control of and accounting for such items. Normally an officer of the counterintelligence unit will be designated as custodian of evidence as an additional duty. For obvious reasons, evidence must be securely stored and protected from the time it is acquired to the time of its use in legal or other proceedings. When applicable, sufficient quantities of evidentiary materials must be acquired to permit laboratory analysis and use in court. For physical evidence to be admissible in a court of law, it is often necessary to establish that the evidence was part of, and found at, a particular place. For this reason photographs should be taken of the scene showing the position of the evidence in relation to that scene. The value of photography as evidence and pertinent rules are discussed in chapter 5.

b. Maintaining the chain of custody of evidence is important in that it permits proof that the piece of evidence collected at the scene is the same as that presented in court, that it was collected at the time specified, and that it was not tampered with or handled by unauthorized persons. The chain of custody is maintained by a receipt system for items of evidence. (DA Form 19–31 (Military Police Receipt for Property)). In addition to DA Form 19–31, classified items will also be covered by a security receipt. The use of DA Form 19–23 (Military Police Property Identification Tag), will provide for easy identification and inventory of property in custody.

c. For transmittal of classified evidence three wrappers should be used.

(1) Inner wrapper. The sealed container is wrapped and properly sealed. The following information should be placed on the wrapper: full address and return address of the transmitting agency; when appropriate, the notation "evidence—to be opened by laboratory personnel only"; and the classification of contents. Except for the addresses, these notations are placed on all six sides of the package. An envelope containing two additional copies of the evidence receipts, two copies of security receipts, plus two copies of the letter of transmittal, should be affixed to the inner wrapper.

(2) Middle wrapper. The package is then wrapped and sealed a second time. The markings are the same as for the inner wrapper except that no notation is made that the package contains evidence.

(3) Outer wrapper. The package is then wrapped a third time and again sealed. The outer wrapper bears only the two addresses. However, a special handling notation must be made if the evidence is perishable, flammable, fragile, explosive, corrotable, or corrosive.

d. The letter of transmittal for shipment of evidence to a laboratory will be prepared in accordance with instructions contained in FM 19–20 and the appropriate PMG technical bulletin. The following items are typical of appropriate data for inclusion in letters of transmittal of this type—

(1) Warning that the package contains evidence.

(2) Brief summary of the case.

(3) Brief history of the evidence.

(4) Specific list of items and their classification.

(5) Clear statement of request explaining reasons for transmittal of the evidence.

(6) Statement as to whether the evidence submitted has already been subjected to examination.

(7) Special considerations or instructions.

4—35. Release of Evidence

Items of evidence will be released or disposed of in accordance with AR 190–22 and, in the case of classified items, in accordance with regulations governing the handling or release of classified material.
Section VIII. THE SPECIAL AGENT AS A WITNESS

4–36. General
AR 381–103 discourages the use of counterintelligence personnel as witnesses at court trials. The regulation requires that prior to authorizing the appearance of counterintelligence agents in legal proceedings related to the results of counterintelligence activities, such appearance will be cleared through the major Army command Staff Judge Advocate. However, infrequently the counterintelligence Special Agent will be called on at a military court-martial, military board proceedings, Federal court trial, or at a foreign court trial to relate certain facts he may have learned during the course of investigation. To be an effective wit-
ness, the Special Agent must be cognizant of what to expect when called to appear, and he must also be familiar with the procedures for taking testimony from a witness.

4–37. Procedures for Taking Testimony

a. Direct Examination. The side which calls an individual as a witness may elicit the information only by a direct examination of that individual. The direct examination has the sole purpose of bringing out the facts within the personal knowledge of the witness so far as that information is admissible under the rules of evidence. In general, the questions on direct examination cannot be leading; that is, they cannot suggest the form of the answer, assume a fact not testified to, or contain a conclusion of counsel.

b. Cross-Examination. After his direct examination, a witness may be cross-examined by the attorney for the opposing side. Cross-examination of a witness is a legal right and its denial is highly prejudicial to a criminal defendant. The purpose of cross-examination is to place direct testimony in its true context to avoid misleading the fact-finding body, and to establish contradictions and improbabilities in the direct testimony in an effort to diminish or destroy the credibility of the witness. If a witness has indicated in a previously sworn statement that one fact exists, and on the witness stand tells a different story, the cross-examining attorney may point out the inconsistency during cross-examination and thereby attempt to impeach the credibility of that witness.

4–38. Appearance of the Special Agent as a Witness

a. Physical Appearance and Demeanor. When a Special Agent is called to appear as a witness, his physical appearance should be faultless, not only in his personal grooming, but also in posture and physical attitude when on the witness stand. He should adhere to all the normal courtesies of the particular tribunal and should maintain a professional manner and bearing. When testifying, he should speak clearly and distinctly so that his testimony will be heard and understood. He must take his time in answering questions, especially during cross-examination, so that he will phrase his reply clearly and concisely, thereby affording the attorney of the side which called him an opportunity to object to a question not proper under the rules of evidence. To be effective and persuasive as a witness, the Special Agent must treat counsel for both sides of the case with equal respect and must not lose his temper, regardless of how trying the questioning may become.

b. Response to Questioning. On both direct and cross-examination, the witness must answer only questions asked by counsel and not volunteer other information. During cross-examination, in particular, the witness should be cautious in responding to questions which might tend to place him in an equivocal position with the intent of diminishing his persuasive effect on the fact-finding body. Ordinarily, the witness must be positive in his answers, testify openly, and admit frankly when he does not know the answer to a question. He should be especially cautious in answering questions involving judgment, such as passage of time, speed of a moving vehicle, distance between objects, and similar questions. Because the answer to such a question is nearly always an estimate or approximation, the Special Agent should phrase his answer so as to make it clear that it is an estimate and not an exact answer. A positive, categorical assertion in answer to such a question may place the witness in a position where he will be made to appear ridiculous under cross-examination. If asked, the Special Agent should acknowledge that he has discussed the case with the attorney of the side which called him as a witness. This is normal procedure and does not imply collusion.

c. Use of Memoranda and Notes. Sometimes a witness does not remember an incident when he is questioned regarding it in a courtroom. He is permitted in such circumstances to refresh his memory from notes, statements, sketches, or other records he may have made at the time of the investigation of the incident. If his memory is refreshed, he then testifies of his independent recollection, answering the question posed. The witness must, however, be prepared to submit such memoranda or notes for inspection by the court of counsel.

d. Classified Information. Legally, if evidence is relevant and material to the prosecution or the defense of a case before a court, board, or other tribunal of the United States, its disclosure cannot be avoided on grounds of security. It is true that courts, boards, or tribunals would not force the individual to commit a violation (unauthorized disclosure of classified defense information), and in most instances the possibility or probability that testimony may involve classified information can be predetermined. In all such in-
stances, guidance must be sought by the Special Agent through his command channels from Department of the Army level. In counterintelligence cases, the decision to prosecute a case or to institute proceedings may involve weighing the effects of information disclosure against security consequences. Normally such a decision would be made at Department of the Army level. In any event, as soon as he can anticipate being called as a witness involving classified information, the Special Agent must seek specific guidance and instructions. A legal proceeding does not relieve the Special Agent of his obligations under the provisions of AR 380–5.

Section IX. SPECIAL SITUATIONS

4–39. Use of Interpreters

Interpreters should not be used in briefing, debriefing, interrogation and interview if Special Agents fluent in that language are available, but in their absence, a properly cleared US or indigenous interpreter may be used. The selection of interpreters should be based on area knowledge, dialect, social status and personality as discussed in FM 30–15. The techniques for the use of interpreters are contained in that field manual. If at all possible, the Special Agent should record on magnetic tape all translations by the interpreter. He should then make random selections of translations for review, comparison, and evaluation at a higher echelon by an American fluent in the language.

4–40. Interviews of Illiterates

Illiterate sources present a problem area for Special Agents. In general, illiterate sources should not be used unless the Special Agent concerned has had experience in handling illiterates. However, many situations will require the use of illiterates, e.g., walk-ins, low level agents, witnesses to incident or personnel security or complaint investigations. Techniques for the interview or interrogation of illiterates are contained in FM 30–15.
CHAPTER 5
TECHNICAL INVESTIGATIVE SERVICES

Section I. GENERAL

5—1. Introduction
Counterintelligence units normally have assigned to them, or available from CI units at a higher level, counterintelligence personnel skilled in audio surveillance countermeasures, defense against methods of entry, investigative photography, and operation of the polygraph. Although these personnel are trained and experienced as counterintelligence Special Agents, the demands for expertise in respective technical skills dictate the need for continued assignment in positions requiring these skills. It is the purpose of this chapter to describe generally the technical areas involved and encountered in counterintelligence operations so that all counterintelligence personnel will have sufficient knowledge in these fields to consider the use of the technical specialist assistance available to them. The employment of such personnel and their skills in support of counterintelligence special operations is discussed in the classified supplement to this manual, FM 30–17A.

5—2. Technical Fields

a. Audio Surveillance. Audio surveillance is the employment of electronic devices for the purpose of monitoring conversation, or other sound, as an aid in the conduct of investigative activities. In the United States and its territories, the use of wiretapping and electronic eavesdropping is strictly limited by the Fourth Amendment to the US Constitution, Section 605 of the Federal Communications Act of 1934, and paragraph 15.11 and 15.220 of the Federal Communications Rules and Regulations. Within the Department of the Army this activity is regulated by AR 381–17. Hostile intelligence services have employed audio surveillance techniques in espionage, sabotage, and subversion against the United States military. These operations must be prevented, or detected and neutralized, if a reasonable degree of military security is to be attained. Audio surveillance countermeasures technical personnel are qualified to conduct both physical and electronic searches for clandestine listening devices, advise commanders on the existence of technical security hazards, and provide technical support of CI operations. A discussion of CI technical surveys and inspections is contained in chapter 11. The legal aspects are covered in chapter 3.

b. Surreptitious Entry. Surreptitious entry is any entry into a guarded or locked area or container and a departure therefrom without leaving a trace that such entry was made. In certain instances, surreptitious entry may violate the provisions of the fourth amendment and constitute a crime under burglary or housebreaking statutes. Persons caught in the course of such entry are liable to prosecution individually. Defense against methods of entry (DAME) technicians are qualified to recognize the relative security factors, delay capabilities, limitations or weaknesses of each type of lock, locking device, locking system, intrusion alarm systems, vault storage area and container, and electronic surveillance devices and systems, e.g., concealed video monitors.

c. Investigative Photography. The overt or covert use of photographic equipment to obtain evidence or information of intelligence value is an important technical investigative method. However, the circumstances involved in setting up the photographic equipment or in getting it into position may constitute a violation of US law, e.g., trespassing or an illegal search within the legal limits of the fourth amendment. Title 18, US Code 2236 is the primary statute of concern to photographic technicians. The local Judge Advocate Office should be contacted if any question exists. Although photographic technicians specially trained in investigative photography and photographic laboratory processing normally are available, all counterintelligence personnel should attain sufficient proficiency in photography to be
able to take acceptable photographs under normal conditions as well as video recordings and reproducing equipment.

d. False Documentation and Secret Writing. Falsified passports, identification cards, and other papers used by hostile intelligence agents to establish their cover and facilitate movement must be detected in order to enhance security. Of equal importance is the detection of secret writing used to transmit information and instructions between enemy agents and their control elements. Technical support and assistance in the detection of these techniques normally are available at the MI unit or higher headquarters.

e. The Polygraph. The use of the polygraph is invaluable as an investigative aid, but it should never be used as a substitute for further investigation. The conditions under which polygraph examinations may be conducted are set forth in AR 195–6. Trained polygraph examiners normally are assigned to military intelligence and counterintelligence units.

Section II. AUDIO SURVEILLANCE

5—3. Audio Surveillance Systems

a. Any audio surveillance device, including those employed by hostile intelligence services, will consist of three basic components—

(1) Pickup device. A typical system involves a transducer, such as a microphone or similar device, to pick up the sound and convert it to electrical impulses.

(2) Transmission link. The impulses created by the pickup device are carried by a pair of conductors, such as wires, conductive paint or tape, directly to the listening post, or to a transmitter which converts the electrical impulses to a modulated radio frequency (RF) signal and transmits the signal to the listening post.

(3) Listening post. The listening post contains the necessary equipment to receive the signals from the transmission link and process them for monitoring and/or recording.

(a) Detection and amplification equipment. Weak signals from the metallic transmission links are amplified and applied to the monitoring and/or recording equipment. Radio signals must first be received on a radio receiver and converted to audio frequency before being applied to the amplifying and monitoring equipment.

(b) Monitoring and recording equipment. Audio signals from the amplifier may be monitored on headphones or by visual indicators and/or recorded on electronic recording devices to provide a permanent record. In special circumstances, the audio from the amplifier may be applied to a higher powered transmitter and retransmitted directly to a remote listening post at an operational headquarters.

b. The components described above are illustrated in figures 5–1 and 5–2. They are available in miniaturized form and can be disguised, concealed, and used in a covert or clandestine manner with variations, limited only by the ingenuity of the technician. They can be incorporated into existing electrical or communications wiring or electronic equipment, concealed in building cavities or conduits, hidden inside office equipment, or placed in furniture or clothing. The listening post can be any secure location from a broom closet to a hotel suite. It may be located within the same building as the listening device, if a metallic link is employed, or it may be in a separate building some distance away, if a radio signal is involved.

5–4. Characteristics of Audio Surveillance Equipment

Items of equipment which can be used in audio surveillance systems vary greatly in size, physical appearance, and capacity. Many items are identical to, and interchangeable with, components of commercially available telephones and radios. Indeed, audio surveillance and countermeasures equipment is available on the open market, although many firms limit the sale to law enforcement or security agencies.

a. Microphones. Microphones can be obtained in practically any size and form. Various types are available for specialized application and may be disguised to appear as such common items as fountain pens, tie clasps, brooches, wristwatches, or various household or office fixtures. Dimensions vary from the relatively large carbon microphones to those as small as 1/4 inch in diameter. Generally microphones must be placed in such a position that air movement generated by sound waves will strike the diaphragm of the microphone. However, access to the area desired may be attained by means of a hollow tube, usually of plastic, which transmits the sound waves to the microphone itself. This tube or the micro-
Figure 5-1. Basic components of audio surveillance wire systems.

Figure 5-2. Basic components of audio surveillance wireless systems.
phone may be concealed behind a wall, under a floor, or above a ceiling, with a small hole bored to permit entrance of sound waves. Another type of microphone, the contact microphone, does not require air movement to actuate the diaphragm, but is placed against a solid which is vibrating as a result of sound waves striking its surface. The solid may be a wall, ceiling, door, window, pipe, or wire conduit which will transmit the vibrations from the desired area to the location of the microphone.

b. Transmission Systems. The simplest transmission system is a pair of metallic conductors to carry the audio from the microphone to the listening post. These conductors may be conventional wires installed and concealed for this specific purpose. Any existing conductors, such as unused electrical wire or ungrounded electrical conduits or similar existing facilities may be used. Special devices such as conductive paint or conductive tape may also be employed as well as existing power or telephone systems. However, wires are not essential. Development of miniature electronic components permits a microphone to be connected to a very small radio transmitter which can be easily concealed. Such transmitters may operate from standard power sources of 110 or 220 volts, or they may be battery operated. Regardless of power source, they are small enough to be concealed easily in floors, walls, electrical outlets, lamp fixtures, or in recesses of upholstered furniture, and may have the capability of remote control to permit operations from distant locations. A battery-powered transmitter may be concealed on a person without being noticeable.

c. Amplifiers. The weak signal from a metallic transmission link must be fed through an amplifier prior to employing monitoring or recording equipment. An amplifier, more correctly called a preamplifier, is normally a solid state miniature device capable of operating for an extended period of time on a set of batteries.

d. Receivers. A receiver is required to detect the signal from a RF transmission link and convert it to audio frequency before it is applied to the amplifier and the monitoring equipment. RF links provided by normal commercial equipment usually employ frequency modulation (FM) techniques. Other forms of transmission include single side band (SSB), amplitude modulation (AM), or pulse modulation. The radio signal may be capable of continuous transmission or remotely keyed. Any radio receiver may be used provided it is compatible with the transmitter. To preclude reception by ordinary household radios and television receivers, transmitters are designed to operate on frequencies not normally assigned to commercial broadcast bands. Receivers are small enough to be carried in briefcases and may be battery operated. They are equipped with earphones as well as with output jacks to permit connecting a recorder.

e. Recorders. Many commercially available wire and magnetic tape recorders may be employed in audio surveillance systems. Some of these have such advantageous features as automatic start and stop (by a sound-actuated relay operating at voice frequencies), extended play and variable tape speeds to permit longer recording time, automatic volume control, and remote control to permit turning off and on from a remote location (by means of a radio signal). Miniaturization of components and use of transistors has led to production of recorders which are extremely light in weight, compact, and self-powered, with extended recording time.

f. Other Items. Cavity resonators (self-contained monitoring units requiring no internal power source) and infrared transceivers (use of invisible beam of light to transmit sound) are no longer new. The use of a parabolic reflector with a microphone attached to a preamplifier to monitor conversations out-of-doors from a remote point is now available. The rapidly advancing state-of-the-art of audio surveillance and countermeasures equipment dictates the need for audio surveillance countermeasures technicians to increase their proficiency by continuous assignment in their technical fields and continued study of new developments.

5—5. The Telephone

Monitoring of telephone conversations is among the most productive means of surreptitious collection of information. Federal statutes regulate the use of electronic eavesdropping devices, and court decisions have held unconstitutional the use of information derived from such devices as evidence. Questions regarding the evidentiary value of information so obtained should be referred to a judge advocate. Frequent use of the telephone tends to reduce alertness to the security threat posed by the instrument. Almost all telephones are susceptible to “bugging” and “tapping.” A “bug” is a modification of the telephone instrument which permits monitoring of both sides of a telephone conversation and also allows the pickup of conversation in the vicinity of the monitored
telephone, even when the handset is on the cradle. “Bugging” may be accomplished by adding of a wire to the existing normal set, internal alteration or modification of the telephone instrument, or concealing a microphone inside the telephone instrument. A telephone “tap” is a device connected to the telephone instrument or line which permits both sides of a telephone conversation to be monitored. “Tapping” may be accomplished by connecting a device to the wires from an instrument at any point along the line, at connector blocks, junction boxes, or the multiwire cables leading to a telephone exchange. A device used for this purpose may be a telephone lineman’s test set, a miniature telephone monitoring device, a radiation type transmitter, or even a telephone number recording device. Indirect tapping of a line (requiring no physical connection to the line itself) may be accomplished by means of an induction coil in conjunction with an amplifier. It must be realized that all of these methods are not readily recognized on sight. The use of technical equipment and a high degree of proficiency are required for the audio surveillance countermeasures technician to check telephones or systems for security. The most thorough check is not absolute insurance against the monitoring of telephones.

**Section III. SURREPTITIOUS ENTRY AND INVESTIGATIVE PHOTOGRAPHY**

5–6. General

a. The DAME technician serves as a security consultant and advisor. He has a thorough knowledge of regulations, directives, federal specifications, and data on locks, locking devices, locking systems, vaults, storage areas, and containers. He is also familiar with foreign locks, although he will require study of the locks in any particular area of operation to perfect his proficiency. His assistance in the planning and execution of CI surveys, inspections, and security spot checks is essential. In case of suspicion of surreptitious entry or in determining the relative security of an area or container, the DAME technician is fully qualified to give expert assistance. While the DAME technician can support the local commander in assessing weaknesses in locking devices, he should not be used as the local locksmith in such services as changing all the lock combinations in the locale.

b. TOE or TD for most counterintelligence units provide for one or more Special Agents highly trained in investigative photography. These technicians are experienced in the use of press and 35mm cameras, 16mm motion picture cameras, video, the Polariod system of photography, microphotography, the latent image silver physical system, and the counterintelligence and intelligence applications of ultraviolet and infrared photography. They are also proficient in laboratory work associated with photography. These technicians are invaluable in training counterintelligence Special Agents in the use of cameras and accessories. TM 11–401 contains basic guidance in photographic theory and the use of photographic equipment.

5–7. Uses of Investigative and Intelligence Photography

a. Investigative Photography. The many uses of photography in counterintelligence investigations include—

1. Identification of individuals. Both overt photography and surreptitious photography are performed in conjunction with surveillance operations.

2. Recording of incident scenes. Both overall views and specific shots of significant items within the incident scene are essential.

3. Recording activities of suspects. Photography is used to provide a record of a suspect’s activities which are observed during surveillance and cover operations.

b. Intelligence Photography. Uses of intelligence photography with which counterintelligence investigators should be familiar include—

1. Overt photography. Photographs innocently taken as private snapshots frequently include information of intelligence value. For example, a street scene snapshot found in the possession of a civilian refugee from a hostile area might include as part of the background a good view of an enemy intelligence agency headquarters—a major CI target.

2. Surreptitious photography. Concealed miniature cameras, microdots, and other surreptitious means are used to obtain and transmit pictures of military installations, items of military equipment, maps, documents, manuals, and other matters of intelligence interest. Advances in the technology of photography, both from the point
**PHOTO DATA CARD**

<table>
<thead>
<tr>
<th>Field</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case Number</td>
<td></td>
</tr>
<tr>
<td>Subject</td>
<td></td>
</tr>
<tr>
<td>Photographer</td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td></td>
</tr>
<tr>
<td>Time of Day</td>
<td></td>
</tr>
<tr>
<td>Weather Conditions</td>
<td></td>
</tr>
<tr>
<td>Camera</td>
<td></td>
</tr>
<tr>
<td>Negative Size</td>
<td></td>
</tr>
<tr>
<td>Lens (Type)</td>
<td></td>
</tr>
<tr>
<td>Focal Length</td>
<td></td>
</tr>
<tr>
<td>Diaphragm Setting</td>
<td></td>
</tr>
<tr>
<td>Shutter Setting</td>
<td></td>
</tr>
<tr>
<td>Film</td>
<td></td>
</tr>
<tr>
<td>Filter</td>
<td></td>
</tr>
<tr>
<td>Camera Positions</td>
<td></td>
</tr>
<tr>
<td>A. Compass Reading</td>
<td></td>
</tr>
<tr>
<td>B. Height</td>
<td></td>
</tr>
<tr>
<td>C. Lateral Position</td>
<td></td>
</tr>
<tr>
<td>D. Tilt</td>
<td></td>
</tr>
<tr>
<td>Artificial Light Used</td>
<td></td>
</tr>
<tr>
<td>Developer</td>
<td></td>
</tr>
<tr>
<td>Developing Time</td>
<td></td>
</tr>
<tr>
<td>Temperature</td>
<td></td>
</tr>
<tr>
<td>Method of Printing</td>
<td></td>
</tr>
<tr>
<td>Contrast</td>
<td></td>
</tr>
<tr>
<td>Type of Enlarger Lens</td>
<td></td>
</tr>
<tr>
<td>Paper</td>
<td></td>
</tr>
<tr>
<td>Distances Between Important Objects in View</td>
<td></td>
</tr>
<tr>
<td>Description of Area</td>
<td></td>
</tr>
<tr>
<td>Remarks</td>
<td></td>
</tr>
</tbody>
</table>

*Figure 5-3. Photo Data Card.*
of view of miniaturization and quality of photography, tend to increase the importance of surreptitious photography to intelligence operations.

c. Photographs of Individual Items as Evidence. Both documents and other physical items of evidence may be photographed in connection with investigations.

d. Specific Techniques for Analysis of Documents. Photography may be used to copy impressions on paper, carbon paper, or chemical erasures. This type of photography normally requires the services of the trained photographic technician and laboratory facilities.

5-8. Photography as Evidence

A photograph may be valuable as evidence since it—

a. Presents facts in pictorial form and creates mental impressions more vivid and realistic than those achieved by words alone.

b. Presents evidence in pictorial form more accurately than the verbal description.

c. Permits consideration of evidence which, because of size, bulk, weight, or condition, cannot be brought into the courtroom.

d. Reduces the need for lengthy descriptions and explanations.

5-9. Rules Pertaining to Photographs as Evidence

In order to qualify for admissibility as evidence, photographs must have been made in accordance with the following general rules:

a. The represented object must be material to the case under trial.

b. The photograph must be free of distortion.

c. The photography must be verified by a person who is personally acquainted with the locality, object, person or thing represented, and who is able to state that the photograph represents the appearance of the subject matter in question.

d. Nothing must be removed or altered at the scene of an incident prior to the taking of the photograph unless absolutely necessary; then a note should be made indicating the reason for the removal or alteration.

e. Although not a prerequisite for admissibility as evidence, photographs should be supported by notes made at the time of photography to provide a description of what the photograph includes, case number of name of the subject, time and date, lighting and weather conditions; plate, film, lens and type of camera; time of exposure and stop used; specific reason for taking the picture; location of the camera; compass direction; and specific reference to all important objects portrayed. Any one of these details may be of importance during a trial, particularly if the photograph is challenged. The notes should be retained by the investigator (photographer) on a format similar to the Photo Data Card as shown in figure 5-3. All photographs must be marked for identification purposes as explained in FM 19–20.

Section IV. FALSE DOCUMENTATION AND SECRET WRITING

5-10. Detection

a. In counterintelligence investigations, particularly in counterespionage and countersubversion, use of false documentation to support cover stories by hostile intelligence agents should be anticipated. False documents are expertly fabricated and extremely difficult for an untrained person to detect.

b. Detection of secret writing, frequently used to conceal messages in innocuous appearing correspondence, is usually beyond the capability of an untrained Special Agent. Suspicion that certain correspondence contains an invisible message may arise, but confirmation, or actual detection, normally requires the services of specially trained technicians and laboratory facilities. Techniques to establish the legitimacy of personal or other documentation, and to detect secret writing may be found in DIAM 58–11 and FM 30–18.

5-11. Availability of Technical Support

a. Personnel trained in detecting false documentation and secret writing may be obtained by counterintelligence elements from higher Military Intelligence headquarters, or through Theater Army. Normally, procedures for obtaining this type of support will be established in SOP.

b. Assistance in detecting false documentation may often be obtained from other intelligence and security agencies, including those of host countries, within the area-of-operations. Such assistance includes information about the types of false documentation which may be encountered, identifying characteristics, and other data concerning the origin and use of these documents.
Section V. THE POLYGRAPH

5–12. General

The polygraph may be used as an investigative aid, subject to the provisions set forth in AR 195–6, to further interrogation or investigation by furnishing indications of attempted deception. Through the employment of proper investigative and interrogation techniques, the polygraph examination of the average subject may provide valuable information. The polygraph will record certain physiological phenomena such as changes in blood pressure, pulse rate, respiration, and skin resistance. The results of a polygraph examination, unless supported by admissions or confessions must be viewed in terms of possibility or, at best, probability of the examinee’s truthfulness. As an aid to interrogation, the instrument has been of considerable value in the field of counterintelligence. Under no circumstances will the polygraph examination be used as a psychological prop. Trained examiners, certified as qualified polygraph examiners by the Department of the Army, are provided in the TOE and TD of most CI units. Counterintelligence Special Agents, however, must be familiar with the capabilities and limitations of the polygraph examination in order to exploit its use properly.

5–13. Objectives of Polygraph Examination

The polygraph examiner attempts to—

a. Ascertain the probability of a person attempting deception.

b. Obtain leads to the facts of an offense, the location of items, and the whereabouts of persons.

c. Compare conflicting statements.

d. Verify statements.

e. Obtain the facts after a test has indicated the possibility that a person is attempting deception.

5–14. Polygraph Examinations

a. General. The examination consists of a pre-test discussion during which the examiner explains the operation of the instrument and reviews the questions to be asked during the examination; the test proper, during which questions to be asked and the subject’s physiological changes to his responses are recorded; and the post-test interview, during which the examiner discusses any problem areas or attempts to determine the reason for questionable reactions or responses.

b. Emotional Factors. Numerous emotions may be involved and will appear on the chart as physiological responses. The chief psychological factor in all polygraph examinations is to focus examinee’s psychological set on that portion of the test which causes him the most concern.

5–15. Suitability of Subjects for Examination

The counterintelligence Special Agent must recognize that certain mental and physical conditions may influence a person’s suitability as a subject for examination and affect his reactions during an examination. The polygraph examiner decides whether or not a person is fit to take the examination, but he does not attempt a psychiatric or medical examination of the subject. It is important that he, as well as the counterintelligence investigators on the case, consider the following:

a. Permanent Physical Illness.

(1) Certain heart conditions and breathing disorders sometimes make a person unfit to take an examination.

(2) A highly nervous or excitable person may be unfit.

b. Temporary Physical Illness. A person who is intoxicated, injured, or suffering pain or discomfort is unfit to be examined. Extreme physical or mental fatigue and certain ills, such as colds, coughing spells, hay fever, asthma, hiccups, and severe allergies, may influence a person’s suitability for examination.

c. Mental Illness. Mentally deficient and insane persons cannot be examined. Persons of very low intelligence may be difficult to examine successfully. Often they display little moral sense or fear of being caught in a lie or an offense. It may be difficult or impossible for them to understand the difference between the truth or a lie, or to understand the purpose and procedures of the examination. If the examiner believes a subject is mentally deficient, insane, or physically ill, he must so inform the agency or office requesting the examination so that action can be taken to have the subject examined by competent medical authorities.
d. Other Considerations. A person who has been treated or questioned improperly prior to the examination may not be a fit subject for the examination. A person who is emotionally upset or under the influence of a depressant, narcotic, stimulant or other drug capable of materially effecting physiological responses, should not be examined while he is in such a condition. A person who is unduly afraid of the test may also present a problem. Proper treatment and a clear explanation of the examination will usually overcome these difficulties.

e. Pretended Ills. Some persons may seek to evade or postpone the examination by pretending a mental or physical illness or some other defect which they feel will make it difficult or impossible for them to be examined.

f. Use of Drugs. The use of certain drugs by a person may affect his reactions on the polygraph. The examiner should be alert for symptoms which may indicate that the subject is under the influence of drugs. When an investigator has advance knowledge that the subject has ingested drugs, he should so advise the examiner prior to the investigation. (See app E for guidance.)

5-16. Treatment of the Subject

Success of a polygraph examination depends in part on how the subject was treated before he was asked to take the examination, the manner in which he was asked to take the examination, and his treatment while awaiting the examination.

a. Routine Questioning. A proper interview seldom affects the examination results. However, the investigator should use common sense as to the length and persistence of questioning. The investigator should not reveal details of an offense to a person who may be asked to take a polygraph examination.

b. Asking a Person To Take the Polygraph Examination. The Special Agent should—

(1) Ask the person to be examined if he is willing to take the polygraph examination and inform him that if he refuses, no adverse action will be taken against him. Further, advise him that no information concerning an individual’s refusal either to submit to or volunteer for a polygraph examination will be recorded in any personnel file.

(2) Attempt no explanation of the polygraph instrument or of the examination as this is the sole responsibility of the polygraph examiner.

(3) Stress the professional qualifications and the impartiality of the polygraph examiner.

5-17. Preparation for a Polygraph Examination

a. Planning Examination Questions.

(1) The examiner prepares the actual examination questions from information provided by the investigator. General facts, theories, and suspicions are not enough; the examiner needs detailed facts.

(2) Whenever possible, the investigator should inform the examiner of the unpublicized facts of the offense, particularly those known only to the victim, the offender, and the investigator.

b. The Setting for Examination.

(1) The examination must be conducted in a quiet, private place. If possible, two rooms should be provided: one as the examination room proper, and the other as a combination waiting room and office. The examination room should be plainly furnished with only a desk, chair for the subject, and chair for the examiner. The subject’s chair should face a blank wall or one free from distractions. The room should be soundproof to eliminate extraneous noises. If the setting is in a warm climate, air conditioning should be installed. A two-way mirror should be placed in one wall to allow for observation when a witness is needed. However, AR 195-6 states that the subject must be informed of the two-way mirror and the existence of audio recording equipment.

(2) The waiting room should contain comfortable chairs, a desk for the examiner, and other equipment which creates a professional impression.

(3) The ideal setting for a polygraph examination will be impossible to achieve in some situations. It is suggested that an effort be made to approach as closely as possible the conditions described above. The examiner will be able to ascertain quickly whether the setting is adequate to permit a successful examination.

c. Arrangements for Witnesses. Normally, only the examiner and the subject should be present in the examination room during the examination. When the subject is a woman, there should be a witness to the examination. Depending on the circumstances, the witness may be present in the room or may observe the examination through a two-way mirror (with the subject’s
knowledge) and listen to the examination by means of a monitoring device (also with subject's knowledge).

5—18. Use of Interpreters

a. At times, the investigator will have to arrange for an interpreter to work with the examiner. The interpreter must be fluent in the two languages to be used so that the translations will be accurate and in the proper idiom. The interpreter should also have some experience in investigative questioning.

b. The interpreter must have a security clearance equivalent to the security classification of the matter to be discussed during the examination or such material as may be revealed as a result of the examination.

c. The interpreter must understand how the examination works and what can be accomplished by it. The examination should be practiced in private until the interpreter thoroughly understand the procedure. The interpreter should be briefed beforehand on the facts with which he must deal in his interpretation.

d. All examination questions should be prepared and translated prior to the examination. Procedures for using an interpreter are similar to those followed in interviews and interrogations except that the interpreter asks the prepared questions at a predetermined signal from the examiner who is operating the instrument.

5—19. Avoidable Mistakes

Most unsatisfactory polygraph examinations are due mainly to unfitness of the subjects and the lack of preparation by examiners and investigators. The Special Agent must bear the following in mind:

a. It is Department of the Army policy that counterintelligence investigations shall be based on evidence, rather than on self-disclosure induced by polygraph examinations. All other investigative techniques should be exhausted prior to granting authorization for the use of the polygraph examination.

b. He must be thoroughly familiar with the case file to include subject’s background. This information, including the dossiers, if available, should be provided the examiner at least two days prior to the polygraph examination, and made available during the examiner’s consultations with the Special Agent.

c. It is imperative to inform the examiner, when known, that the subject is overly emotional, uses alcohol to excess, may be under the influence of sedatives or drugs, may be addicted to narcotics or marijuana, suffers some mental aberration, or possesses other disabilities or defects which may cause abnormal responses.

d. He must consult with the examiner when in doubt as to the person's fitness to take the examination. If there is still doubt, consult the individual exercising command or operational supervision for further determination and appropriate action.

e. He should never describe the polygraph instrument as infallible.

f. The polygraph is used solely as an investigative aid and does not determine guilt or innocence.

5—20. Reports, Records, and Charts

a. Reports and Records. The report forms to be used, records to be maintained, and distribution are prescribed in AR 195–6. The Special Agent will coordinate with the examiner in the preparation of portions of the form having to do with the background of the investigation.

b. Polygraph Examination Results. Polygraph examination reports obviate the necessity for preparing a detailed Agent Report, DA Form 341, except that the Agent Report may be used as a cover sheet to transmit the material. No mention of the results of the examination or of the information obtained will appear in the Agent Report (chap 7).

c. Statistical Data. Polygraph examiners will maintain monthly statistics of all examinations conducted. The data collected will not contain the names of persons examined. In addition, a log of persons examined, by name, may be maintained provided that the results of the examination are not indicated or keyed to the names.

d. Statement of Consent. The Polygraph Examination Statement of Consent (DA Form 2801) will be read and signed by each person prior to submitting to polygraph examination. Prior to signing the statement, examinees must be given an explanation of rights under Article
31 of the Uniform Code of Military Justice and the Fifth Amendment to the Constitution and their right to counsel (chap 3) since the answers to the examiner's questions can be introduced into evidence against him. This is not to imply that polygraph examinations are admissible which would be an incorrect assumption. Polygraph examinations are not reliable enough to be admissible in a court of law. The procedures outlined in AR 195–6 apply.
CHAPTER 6
SOURCES OF INFORMATION

Section I. GENERAL

6–1. Introduction

The counterintelligence mission requires the continuous availability of sources of timely and reliable information on individuals, groups, and organizations which pose a security threat to the military establishment. One of the counterintelligence Special Agent's most effective means of obtaining the required information is through knowledge and exploitation of the sources of information available to him.

6–2. Sources of Information

A “source of information” is defined for purposes of this manual as any person, thing, or activity from which intelligence information is obtained. All sources fall into one or more of the following three categories—human, documentary, and technical/materiel.

Section II. HUMAN SOURCES

6–3. General

Among the Special Agent's most valuable sources of information are people. Whether their attitude is friendly, hostile, or indifferent, the ability to exploit those persons who possess or can obtain information of CI interest requires a special investigative proficiency that must be developed by all professional counterintelligence personnel.

6–4. Conventional Source

A conventional source is an individual with whom unconcealed, normal, overt contact is maintained. This type of source may provide any type of intelligence information; under normal circumstances, his identity, relationship, and connection with US intelligence will not jeopardize him in any manner. If the source repeatedly furnishes privy information, the source’s identity in counterintelligence reports may be concealed in order to protect the flow of information and insure continued usefulness. Conventional sources are divided into the following classifications:

a. Incidental Sources. Individuals who furnish information either on a one-time basis with no intention of repeating this service or who furnish information on an infrequent and irregular basis which does not meet the criteria for classification as a “casual” source are known as incidental sources. These include—

(1) Interviewees. Individuals contacted by Special Agents or summoned to a counterintelligence office during the course of an investigation for the purpose of being interviewed and who are aware that they are in contact with an official military agency are termed interviewees.

(2) “Walk-ins” or volunteers. Individuals who, of their own accord, contact a counterintelligence office in order to divulge information they believe to be of CI interest are termed “walk-ins” or volunteers. This category includes well-meaning, patriotic citizens who furnish valuable information, but also encompasses a wide range of persons motivated by malice, avarice, revenge, or jealousy, who may volunteer biased, distorted, or completely false information for personal reasons. Hostile intelligence agencies may also sponsor confusion agents who act as “walk-ins” to disseminate false or misleading information. Determination of the true identity and motives of “walk-ins” is essential to the evaluation of any information they may offer (para 4–13).

(3) Unwitting sources. Individuals who provide information of CI interest without being aware that they are imparting such information are termed unwitting informants. Information may be obtained from such persons by subtle elicitation techniques or through technical surveillance.
(4) **Others.** Any individual, by virtue of his position and knowledge, may possess vital or special information of CI interest. Normally, such sources are contacted for a specific purpose and continuous contact is not anticipated. The information provided may be either wittingly or unwittingly disclosed by the source, and the nature and circumstances of the type information obtained determine the need for protection of his identity. These types of incidental sources are—

(a) Defectors.
(b) Escapees.
(c) Refugees and displaced persons.
(d) Repatriated personnel and expellees.
(e) Detainees.
(f) Captured enemy personnel.
(g) Expatriates and members of minority groups.

(h) Tourists and other transient personnel.

(i) Attendees at international gatherings.

(j) US citizens living abroad.

(k) Local nationals employed by US forces.

(l) US military personnel, active, reserves, or retired, and their families.

b. **Casual Sources.** A casual source is one who, by his social or professional position, possesses or has access to information of continuing interest, and who willingly provides this information to the counterintelligence unit, either in response to a specific request or on his own initiative. A casual source is under no obligation to furnish information and normally is subjected to only as much control as he is willing to accept. He usually can be relied upon only for that information which is routinely available to him, and normally there is no assurance that he would not furnish the same information to any other agency requesting it.

c. **Official Sources.** Individuals who, by virtue of their official positions, are expected or obligated to provide intelligence information openly to counterintelligence units in the normal course of their duties are termed official sources. Certain government officials, police officers, and technical experts are examples of official sources. Foreign government officials and representatives may also fall within this category, depending upon the circumstances and agreements in effect. Continuing contact with official sources over a period of time will frequently result in a relationship where the degree of cooperation with the counterintelligence unit extends beyond that inherent in the official's position. In such cases, measures must be taken to protect his connection and identity with the information provided.

### 6–5. Confidential Source

A confidential source is an individual whose identity and association with US intelligence for personal, business, official, or other reasons must be afforded security protection. In the field of counterintelligence, confidential sources are generally employed in special operations, counterespionage, countersabotage, and countersubversion activities. Confidential sources used in counterintelligence special operations must be administered and registered in compliance with appropriate directives. For a detailed explanation of confidential sources, see FM 30–17A.

#### Section III. DOCUMENTARY SOURCES

### 6–6. General

A document is defined as any written, drawn, or printed material which conveys information. The ability to exploit available documentary sources is an investigative technique that provides a wealth of intelligence information, and greatly reduces the time and effort expended in counterintelligence investigations and operations. Documentary sources include mass media, scientific and technical material and correspondence or other documents exchanged between individuals, agencies, and governments as well as documents captured by US forces or obtained from friendly forces.

### 6–7. Mass Media

Mass media documentary sources are those readily accessible to the general public and, in most instances, easily obtained. Routinely available publications, both domestic and foreign, should be utilized by the Special Agent in order to keep well informed of current world and local events, trends, political movements, personalities and organizations. Newspapers and news magazines; telephone, city, business and professional directories; maps; town plans; gazetteers; trade journals; transportation listings, schedules and routes; and standard references such as "Who's Who," almanacs and encyclopedias are some of
the publications available. Propaganda efforts of hostile and opposition forces, such as leaflets, newspapers and magazines, and trade publications, also assist in planning and conducting counterintelligence investigations and operations. The mass media approach to the collection of intelligence information requires a great deal of manpower and time to evaluate the worth of the material. Differences between developed and underdeveloped societies usually mean a corresponding difference in the quantity of publications that might provide information concerning the workings of a society and its people.

6-8. Scientific and Technical Documents/Data

Exploitation of documents and data pertaining to scientific and technical matters may reveal advances and weaknesses of a country. FM 30-16 contains guidance on the handling of scientific and technical documents.

6-9. Correspondence, Documents and Records

Perhaps the most widely and often used type of documentary source is correspondence or other documents legally and overtly exchanged between individuals, agencies and governments. As explained in chapter 4, the files and records maintained in the offices of the numerous federal, state, and local agencies, both military and civilian, are constantly utilized by the Special Agent during the course of investigations. Counterparts of our national, local, state, and private agencies also exist in most overseas areas. Although the scope and operations of these various overseas agencies will vary from their American counterparts, in most cases, their recorded information will parallel or even exceed that information available in similar agencies in the United States. The reliability of recorded information obtained from overseas agencies will vary depending upon the country and agency involved. Such information must be closely analyzed and evaluated before being accepted as established evidence or fact. Important sources of information to the Special Agents are those documents obtained from local and higher intelligence headquarters; these include such publications as intelligence summaries (INTSUM), periodic intelligence reports (PERINTREP), intelligence studies, directives, and SOPs. Through judicious use of available records and files, investigation can be reduced greatly and information verified. Leads can be provided indicating the existence and location of information which can be exploited.

Section IV. TECHNICAL/MATERIEL SOURCES

6-10. General

Technical devices or equipment, materiel, or physical items that can be exploited for investigative purposes are valuable sources of information to the Special Agent. Common sources are ordinary AM or FM radio broadcasts and telecasts. Additional sources include photographs or films, tape recordings, and charts (chap 5).

6-11. Technical Intelligence

Whenever captured or confiscated equipment or materiel used or manufactured by foreign nations comes to the attention of counterintelligence personnel, the item should be examined for possible counterintelligence use and then turned over to the technical intelligence unit for exploitation (FM 30-16).

Section V. LIAISON

6-12. General

a. Inherent in the exploitation of sources is liaison between individual parties or organizations to insure mutual cooperation, understanding, and unity of purpose and action. In CONUS, and particularly in overseas areas, liaison with the agencies and individuals having records and information of CI interest is essential to the success of counterintelligence investigations and operations.

b. The nature of counterintelligence activities and the many legal restrictions imposed, particularly by status-of-forces or other delimiting agreements, frequently make the collection of counterintelligence information dependent to a large extent upon the effectiveness of liaison. Liaison with appropriate US, host country, and allied military and civilian agencies is fundamental to the success of counterintelligence operations. Liaison procedures should be established by unit SOP. Frequently the employment of a full-time liaison officer, or section, to maintain regular con-
Contact with designated military and civil agencies will be necessary.

c. In addition to national agencies maintaining or processing records and information of CI interest, there exists numerous local agencies which may also provide assistance to CI activities and operations. Counterintelligence personnel must be familiar with available agencies and the type and scope of information which they can provide. Chapter 4 discusses the principal types and locations of pertinent records that will often be of CI interest.

6-13. National Agencies in CONUS

Liaison activities at the national level with military, Department of Justice, Treasury Department, State Department, Central Intelligence Agency (CIA), Civil Service Commission, Veterans Administration (VA), and the Office of Selective Service are normally conducted at Department of Defense or Department of the Army level. Information contained in the reports and files of these agencies is usually received as a result of a National Agency Check (NAC). For further information, see FM 30–17A.

6-14. Local Agencies in CONUS

Liaison with military, civilian, private agencies, and with offices of national agencies at local levels is usually accomplished by a Special Agent designated by his unit to establish direct, personal contact. In addition to Federal agencies represented at the local level, other agencies that should be contacted include:

a. Military G2/S2, personnel sections and provost marshals of units in the area.

b. Civilian agencies such as state and local police or sheriffs’ offices, bureaus of vital statistics, state crime commissions, state adjutants general, state boards of education, motor vehicle bureaus, and local courts.

c. Private agencies such as chambers of commerce, credit agencies, and public utilities.

6-15. Agencies Overseas

a. Liaison is essential to the success of counterintelligence exploitation of information in overseas areas of operation. Many US agencies and counterpart agencies of host country and allied forces will be found in overseas areas.

b. Personnel engaged in liaison activities must be aware that, whether of an official or informal nature, liaison is a two-way street. The person contacted by the Special Agent is usually from some other intelligence, law enforcement, or security agency, US or foreign, and expects to receive information from the Special Agent as well as to provide information. Counterintelligence personnel involved in liaison duties must be familiar with pertinent local directives and SOP, A 380–5, AR 381–115, and other pertinent ARs of the 380- and 381-series. The general rule ("third agency rule") is that information will not be passed to another or third agency without the consent of the originating agency. Liaison positions differ in complexity from those involving only records checks or exchange of documented material to those involving detailed coordination of all types of counterintelligence investigations and operations. The skilled liaison officer must recognize his own limitations and bring other counterintelligence personnel into contact with other agencies when the occasion demands.

c. Additional overseas agencies include:

(1) US official agencies.

(a) US embassies, legations, or consulates.

(b) Other intelligence and tactical units in the area.

(c) Local Judge Advocate General offices.

(d) Intelligence advisors to host country military forces.

(e) Special Forces units.

(f) Military Assistance Advisory Groups (MAAG).

(g) Labor service battalions.

(h) US Operations Missions (USOM).

(i) Civil Affairs units or staff sections.

(j) Psychological warfare elements.

(k) Provost Marshal and US Army Criminal Investigation Command (USACIDC).

(l) USASA units.

(2) Host country official agencies. Regardless of the status of US elements in the host country, liaison personnel must exert all possible efforts to establish personal rapport with their military and civilian counterpart agencies at national and local levels. In overseas areas, liaison functions normally are assigned to full-time liai-
son personnel who should possess local language capabilities, have broad professional background, and possess personal characteristics of maturity and good judgment.

(3) **Allied forces.** When US forces are engaged in tactical operations in conjunction with armed forces of allied nations, close and continued liaison must be established with the respective counterintelligence and other intelligence agencies.
CHAPTER 7
INVESTIGATIVE REPORTS

Section 1. INTRODUCTION

7-1. General
The information obtained through application of the various investigative techniques and procedures will be of little value unless it is accurately recorded and reported. In general, counterintelligence reports are written to transmit information to an action agency, serve as a source of information for intelligence research, and serve as a permanent record of investigation. Since the end product of any investigation performed by counterintelligence personnel is the written report, a system of standardized counterintelligence investigative reports is used to insure the logical presentation of specific information gathered. Sample investigative reports of all types are provided by command or intelligence unit SOP; samples of pertinent reports are included in appendix B to this manual as well as details on how to complete them correctly.

7-2. Types of Reports
There are five basic forms of counterintelligence investigative reports. Forms to be used in reporting polygraph examinations are described in AR 195-6 while special operational reports are contained in the classified supplement to this manual, FM 30-17A.

a. DA Form 341 (Agent Report)—DA Form 341 is the primary report form for recording results of counterintelligence investigations.

b. DA Form 342 (Report of Investigation)—Accumulated Agent Reports and exhibits for a single investigation will be compiled and results forwarded by DA Form 342 (ROI).

c. DA Form 568 (Summary of Information)—A brief narrative, sufficiently detailed to enable the reader to understand what is contained in other investigative records and reports, is forwarded on DA Form 568 (SOI).

d. DA Form 2784 (Request for and Results of Personnel Security Action)—DA Form 2784 is used by authorized requesters to request a background investigation and by control offices to notify requesters of the results of investigation.

e. DD Form 1584 (Department of Defense National Agency Check Request)—DD Form 1584 is used by authorized requesters to request the conduct of a NAC, regardless of whether or not the NAC is a component of a background investigation.

7-3. Basic Characteristics of Reports
The secret of writing good counterintelligence reports lies in the writer’s ability to pay strict attention to details. Attention must be given to the application of the six standard characteristics of all good reports.

a. Accuracy. Accuracy is the most important characteristic. Reports must reflect exactly what was seen, heard, or done. The Special Agent must not make assumptions, interpret information, nor draw conclusions. When a source expresses an opinion or belief, it should be reported as such, and not as a fact. Accuracy also means precision (i.e., correct spelling of names, business firms, and cities; exact reporting of dates, addresses, and times; and careful descriptions of actions, comments, and records).

b. Completeness. If even one small link in the chain of facts is omitted, those who must take action on the report may make the wrong decision. So far as possible, the six basic interrogatives (who, what, when, where, why, and how) must be answered in relation to every phase of the report. To insure against omissions, the report should be proofread carefully and compared with the notes on which it is based after the report is finished.

c. Pertinency. Pertinency means that the information recorded in the report has a direct bearing on the purpose of the investigation. Only information that is relevant to the investigation should be included in the report.
Section II. PURPOSE AND USE OF COUNTERINTELLIGENCE INVESTIGATIVE REPORTS

7—5. General
Subsequent paragraphs will discuss the five basic counterintelligence forms in use in the US Army and their purpose and use. Details on how to complete these forms are contained in appendix B, or in AR 381–130.

7—6. The Agent Report (DA Form 341)
The Agent Report is used to record information obtained as a result of counterintelligence investigative activities conducted by one or more Special Agents in connection with personnel security investigations or incidents, and obtained through interview, interrogation, observation, surveillance, records examination, or other special investigative techniques. Normally, each single investigative activity will be reported on a separate Agent Report. Agent Reports serve as the basis for other counterintelligence reports such as the Report of Investigation and Summary of Information. Therefore, Agent Reports must contain sufficient information in proper form to justify any resultant action, and they must answer any reasonable questions which might be raised by authorities reviewing the case. It is the responsibility of the Special Agent to develop fully and record accurately and impartially all pertinent information, both favorable and unfavorable, to preclude incorrect or arbitrary conclusions by a reviewing or action agency. However, Agent Reports will not be passed outside of MI channels.

7—7. Report of Investigation (DA Form 342)
The Agent Report and exhibits accumulated as a result of specific investigative activities conducted during the course of an investigation will be compiled and a synopsis of their content prepared. These three elements—synopsis, Agent Reports, and exhibits—are combined to form a Report of Investigation (ROI), which is a complete account of either the entire investigation or particular portion of the investigation. The synopsis will be prepared on the ROI, to which the Agent Reports and exhibits are attached. The synopsis allows the requester or action agency to study the investigation systematically and then base its decision upon the findings. Reports of Investigation are prepared by the control office for the investigation under the following conditions:

a. Upon completion of:

(1) All CTIs.
(2) All personnel security investigations which result in evidence deemed sufficient to war-
rant recommendations adverse to the interest of the person investigated.

(3) All personnel security investigations of such importance or complexity that it is felt that DA Form 2784 (Request for Results of Personnel Security Action) would not furnish an adequate summary of the rests.

b. Prior to the completion of an investigation:
   (1) In urgent situations which require immediate precautionary or preventive measures.
   (2) In cases of treason, espionage, sabotage, or sedition, when the initial ROI is prepared within 30 days of initiation of the investigation, regardless of the status of the case. Subsequent reports of investigation will be submitted as necessary and upon completion of the investigation.
   (3) Whenever the investigation is suspended, canceled, or transferred to another jurisdiction.

7—8. Summary of Information (DA Form 568)
The Summary of Information (SOI) is used to present a concise history or summary of the information available concerning an individual, organization or an incident. A SOI may be used as a basis for some decisions (e.g., a decision to initiate an investigation), but is never used as a basis for direct action against an individual. It is used as a means of transmitting information between commands and offices, including counterintelligence offices. It is not intended to replace other forms, such as the ROI, Agent Reports, or Lead Sheet, and it is not used to report original information. The SOI normally is used to transmit the following types of information:

a. A summary of files or records.

b. Information which is considered of importance to any government agency which has a proper interest in the facts.

c. Characterizations are biographic sketches of individuals or organizations who routinely service Army installations or make requests to Army elements and officials. These requests may be for a variety of reasons. For example, requests may be for admittance to installations as for civic support, speakers, autographs, drill teams, bands, and even escorts for festivals and homecomings. In these cases, characterizations may be requested for use in determining the appropriate response or course of action.

7—9. Request for and Results of Personnel Security Actions (DA Form 2784)
Request for and Results of Personnel Security Action (DA Form 2784) provides a standard format for requesting a background investigation, limited investigation, review of previous investigations in order to validate an existing clearance, or a check of intelligence files for any purpose. Its use is restricted to actions involving individuals. Control offices will utilize DA Form 2784 to notify requesters of the results of investigation. When the results of a background investigation are completely favorable, the investigative reports will not be furnished the requester (action agency) unless specifically requested. This form will not be used to request a National Agency Check (NAC) or Entrance National Agency Check (ENTNAC) only. (See AR 381-130 for distribution and instructions for completion of DA Form 2784.)

7—10. Department of Defense National Agency Check Request (DD Form 1584)
Department of Defense National Agency Check Request (DD Form 1584) will be used to request, control, conduct, and return results of a National Agency Check (NAC) or Entrance National Agency Check (ENTNAC). For details in purpose, preparation, and distribution, see AR 381-130.

7—11. Spot Reports
In addition to the five basic investigative reports, any information obtained by counterintelligence personnel which requires immediate dissemination to user agencies (tactical or nontactical) will be submitted so that the responsible command and, if appropriate, Headquarters, Department of the Army, may be promptly advised. Transmittal of such information is normally in the form of a spot report (AR 381-130).
CHAPTER 8
PERSONNEL SECURITY INVESTIGATIONS

Section I. GENERAL

8—1. Purpose
Security regulations, particularly AR 380–5, governing classified material and information provide that no person is entitled to knowledge or possession of classified defense information or material solely by virtue of his grade and position; that such will be entrusted only to those individuals whose official duties require access to such knowledge; and that all such persons be cleared to receive this material or information on a "need-to-know" basis. One means employed to protect classified defense information and material from unauthorized disclosure is the conduct of personnel security investigations of those persons who have or will have access to classified defense information. This is done to insure that personnel concerned are of unquestioned loyalty, integrity, and discretion; of excellent character; and of such habits and associations that no doubt exists concerning their ability and judgment in properly handling such information.

8—2. Types of Personnel Security Investigations
Personnel security investigations are of two types: National Agency Check (NAC), and Background Investigation (BI). The type and scope of investigation required in any instance will depend upon the category of classified defense information to which a clearance for access is required and on the citizenship status of the individual concerned. General principles, supervision, control, and procedures governing the conduct of these investigations are contained in AR 381–130 and AR 604–5. When personnel security investigations are conducted on foreign nationals in overseas areas, the scope of investigation will be prescribed by the responsible area commander. Chapter 7 and appendix B describe procedures used by counterintelligence personnel to report the results of personnel security investigations.

Section II. CONDUCT OF BACKGROUND INVESTIGATIONS

8—3. Scope of Background Investigation
a. Most counterintelligence investigations are background investigations (BI). Their scope encompasses fourteen component parts and generally covers the last 15-year period of the individual's life to the date of the investigation, or from the subject's 18th birthday to the date of investigation, whichever is shorter.

b. The education and birth records checks, which are considered important parts of the BI, are conducted without regard to the time and date of birth limitations indicated above. The restriction on the 15-year coverage, or the individual's 18th birthday, concerns the Special Agent only in that he is not required to deliberately seek information not within the usual period of coverage unless a discrepancy develops during the investigation.

c. There are times when the period of coverage may be extended to any period of the individual's life:

(1) In the event that such a step is necessary to substantiate or disprove derogatory information.

(2) When extended coverage is required by competent authority.

(3) When the individual is 17 to 19 years of age (the investigation will embrace coverage back to age 15).

8—4. Components of a Background Investigation
There are fourteen minimum components or requirements of a BI, all of which are significant in determining an individual's loyalty and suitabilit-
ity. These components are prescribed in AR 381-130 and AR 604-5 and are discussed individually below.

8—5. National Agency Check

a. A National Agency Check (NAC) consists of a search of the records and files of appropriate national agencies for information bearing on the loyalty, trustworthiness, and suitability of individuals under the investigative jurisdiction of the DOD establishment. Whether used as the basis for a clearance or as a part of a BI, the procedure is the same. The types of National Agency Checks, national agencies of concern, location of specific records, conditions under which these records will be examined, and pertinent administrative instructions are described in detail in AR 381-130.

b. The designation and processing of NACs are administrative responsibilities of the control office; however, if during the course of an investigation there is indication that additional specific agencies should be checked, the Special Agent should recommend that such checks be made.

c. The control office will extend the inquiry to obtain additional information as necessary in the event that derogatory or adverse information is received in reply to an inquiry or developed during the conduct of the investigation.

8—6. Birth Records

Examination of birth records is normally not included in a BI. If, however, in the course of the investigation a discrepancy is noticed in the date and place of birth as listed by subject on his DD Form 398, (Statement of Personal History), special effort is made to determine which information is correct. In establishing the correct date and place of birth, the best information is obtained from an official birth certificate or vital statistics records maintained by municipal, state, or other government agencies. The appropriate agency varies in different areas. Birth records may be kept by a bureau of vital statistics, department of health, or similar agency, and may be maintained at state, county, city, or township level. Other methods of verifying birth information may be resorted to when no official records are available. In such cases, the investigator attempts to find the best information obtainable. Records of doctor, midwife, or a hospital may be used. The vital statistic files of a newspaper which carry birth announcements, especially in rural areas, may be accepted. Baptismal and church records may provide verification, as would entries in an old family Bible. In cases of adoptions or of illegitimate births, the verification may require a check of court records, or interviews with parents, guardians, or lawyers. In verifying birth data, the Special Agent must be careful that the information obtained is a verification and not merely a repetition of the original source of information.

8—7. Education

a. Time spent in high school or college represents a formative period of an individual's life, and much can be learned which may not be reflected in the school records. It is important that in addition to a check of school records, personal interviews be conducted with teachers or others connected with the school who may have an intimate knowledge of the subject's activities. Teachers at high school and college level generally have about four different classes every day, and the composition of these classes usually changes every 6 months. It can be expected that a teacher may not be certain that he knows the subject. Most schools publish yearbooks with individual photographs of students which can be used as an aid in identification. Some teachers may have more significant information than others, and these should be searched out. The Special Agent should not be satisfied with broad statements such as "John was a good student," or "George showed subversive tendencies." He must obtain facts and details; he should determine what the subject said or did that led to a conclusion concerning his character, integrity, and loyalty. In some areas, juvenile delinquency is not recorded on criminal records, but it may be found in school records.

b. Extracurricular activities, as well as academic achievements of the subject, should be considered. Not only the names of organizations, but the subject's degree of interest and participation should be determined. Mere membership in a subversive organization is not conclusive evidence of disloyalty. For example, some individuals are "professional joiners" and become affiliated with every club, society, or activity possible. Often they have little idea of the purpose or functions of these organizations and may have become members of subversive or front organizations without actual knowledge of that fact. No conclusive opinion can be based on the mere fact of membership in such an organization. The Special
Agent should intensify and extend the investigation so as to prove or disprove any alleged subversive connections of the subject. Among the facts to be determined are subject’s contributions, activities, degree of association, and acceptance of the organization’s principles.

8—8. Employment

Employment records are examined in order to verify the period of employment and to determine details regarding the subject’s duties and general reliability. The reasons for termination of employment are significant. Data extracted from employment records should be substantiated by obtaining additional information from individuals familiar with circumstances reflected in record entries, e.g., a coworker, supervisor, or employer. In addition, such persons may provide information concerning subject’s loyalty, character, behavior traits, and reputation. Unions and labor activities are primary targets for subversive elements, and subject’s participation in union activities may provide information concerning his particular views and attitudes. However, membership in a union known to have been infiltrated by subversive personnel is not in itself evidence that the subject subscribes to objectives inimical to the United States. In such instances, an extremely careful and sensitive investigation of the subject’s participation and affiliation in union activities is essential, in order for responsible authorities to reach objective and valid conclusions concerning its significance.

8—9. References

It can be assumed, in most cases, that listed references will be prejudiced in favor of the subject. Obviously, the subject selects as listed character references those people on whom he can best rely to furnish favorable information.

a. Listed references may unwittingly reveal derogatory or adverse information during the interview concerning subject’s background, character, or activities, thinking that they are flattering the subject.

b. Listed references are usually sources of leads to individuals who have knowledge of subject’s background and associates, but who are not listed as references.

c. Listed and developed character references are also the best sources for obtaining information regarding spouses, former spouses, or children, etc., who may be, for various reasons, omitted from DD Forms 398. Relatives of subject will not be interviewed as listed or developed references unless special circumstances warrant.

d. Most people, when told the subject is under consideration for a position of trust and responsibility with the US Government or the Army, feel a moral obligation to be truthful. They are frequently more honest in appraising a subject than he may have anticipated when he listed them as references.

8—10. Neighborhood or Residence Investigations

The interview of persons residing in the vicinity of the subject’s residence may be conducted when considered necessary to the completion of the investigation.

8—11. Criminal Record

When appropriate, or when information developed from a NAC is not considered adequate, it may be necessary to check the records of police departments and other law enforcement agencies in the vicinity of subject’s past and present residences and employment. Such checks are commonly referred to as local agency checks. In all records checks, attempts are made to substantiate or verify the recorded information with testimony, evidence, and statements. Police records may show possible involvement in a crime, but court records may reveal that the subject was acquitted. On the other hand, acquittal may be based upon a legal technicality or upon a faulty indictment. Scrutiny of the actual trial record is important to obtain significant information; it may be derogatory to the subject or provide leads for further inquiry. While the Special Agent seeks the best evidence, facts, and definite information, he is also interested in rumor, hearsay, and opinion, if they are pertinent to the investigation and lend themselves to further development as leads.

8—12. Military Service

The service of an individual in the Armed Forces, and the type(s) of discharge will be verified. The verification of an individual’s present service is accomplished by a check of the local and major unit’s personnel files and by interviewing the immediate supervisor and coworker when required. Past service and type(s) of discharge received are components of the NAC and will be accomplished by the control office. It is possible under
certain circumstances to execute administrative discharges for such activities as disloyalty, subversion, indiscretion, or moral turpitude, and such discharges may not be honorable. It is, therefore, imperative that discharges not only be verified but the circumstances of the discharge be investigated.

8—13. Foreign Countries
Both the material and personal interest an individual may have in foreigners or foreign organizations, either domestic or abroad, must be considered during the investigation, since coercion or pressure may be put upon such an individual through foreign relatives or investments. This does not necessarily indicate that an individual is untrustworthy, but it is a factor to be considered for the protection of both security and the individual.

8—14. Citizenship Status
The citizenship status of the individual must be established in every BI. In all cases where the subject is not a natural born United States citizen, the investigation should show whether he is a naturalized citizen, holds derivative citizenship, or is an alien.

(a) United States citizenship may be acquired in three ways—

(1) Citizenship by birth. Records check of the individual's birth will establish this type of citizenship.

(2) Naturalized citizen. When the individual or his parents are naturalized citizens, the date and place of birth, as well as naturalization of the individual, are verified through records of the appropriate US District Court. If the place of naturalization cannot be determined, Immigration and Naturalization Service (INS) records, Washington, DC, are examined. Citizenship itself is not awarded by the INS, but is normally granted in a Federal or state court.

(3) Derivative citizenship.

(a) If a minor is brought into the US by his parents and the parents obtain US citizenship prior to the child's 18th birthday, the latter may claim derivative citizenship.

(b) An individual born outside the US, but whose parents are US citizens, may have dual citizenship. However, he can renounce citizenship of the country where born and claim US citizenship based on his parentage. He should have proof in the form of a “certificate of citizenship.”

(b) In verifying citizenship, the Special Agent should be familiar with the terms “alien” and “immigrant alien.”

(1) An alien is any person who is not a citizen of the US.

(2) An immigrant alien is an alien who legally entered the US under an immigration visa for permanent residence. During a BI, the alien registration records will be checked at the INS District Office in the area that subject currently resides in, to verify the date and place of legal entry into the US. If subject has moved to this residence since 1 January of the current year, the records of the INS, Washington, DC should be searched to obtain the required information.

8—15. Foreign Travel
If an individual has traveled outside the US within the last 15 years, except in military service, or while the dependent of persons in such service, records of the Department of State will be checked to determine the reasons for travel.

(a) Department of State records may have such information as dates of departure and return, destination and possible activities in which the individual was involved while abroad.

(b) The Central Intelligence Agency (CIA) may have information on foreign travel, activities, and connections of US citizens. However, their files do not antedate July 1946.

8—16. Credit Records
Whenever necessary, credit agencies and credit references will be checked. Credit record checks are made to determine the integrity and suitability rather than the loyalty of the individual. The investigation should be expanded if an indication of bad credit or lack of financial responsibility is revealed. All bad credit references obtained from financial institutions which were obtained from other firms should be checked with the reporting firm since errors do occur or the subject may have had a legitimate complaint which was later settled.

8—17. Organizations
(a) When it is determined that the subject of a BI had or has affiliation or sympathetic association with subversive type persons or affiliation with, or membership in, subversive organizations as explained in AR 381–130, this association will be established in fact and included in the Agent Report of the BI.
b. Subversive elements make concerted efforts to infiltrate and penetrate all groups and organizations, to include educational institutions, labor unions, veteran groups, and fraternal organizations. In view of this fact, all such associations by the subject should be reported. This serves not only to determine subject's friends' associates, and possible activities or ideologies, but also to provide a reference for future checks should any of these organizations later be determined to have subversive tendencies or membership.

c. The frequent explanation that participation in subversive activities was due to immaturity, misplaced ideals, exercise of intelligence freedom, youthful impulsiveness, etc., is no basis for failure of the Special Agent to report such information. The Special Agent must report all information reflecting on the subject.

8–18. Divorce Records

Appropriate court records will be reviewed for verification of pertinent information when the subject has been divorced. Further investigation may be conducted when essential to fair and proper resolution of the case.

8–19. Derogatory Information

a. Suitability. If, during the course of a BI, credible information is received or developed which reflects adversely on the character, integrity, morals, or discretion of the subject, the control office may change the case category to that of an expanded BI. AR 604–5 lists a number of suitability criteria; but information indicating that the subject has engaged in conduct falling within these criteria does not necessarily mean that he is unsuitable. It is only upon completion of appropriate inquiry of investigation and review of all pertinent facts that a positive determination can be made.

b. Loyalty. If, during the course of a BI, credible information is received or developed which reflects adversely on the subject's loyalty to the US, the control office may change the case category to that of a CTI. Chapter 9 explains the types and conduct of CTI.
CHAPTER 9
COMPLAINT TYPE INVESTIGATIONS

Section I. GENERAL

9–1. Definition and Purpose
A complaint-type investigation (CTI) is one in which sabotage, espionage, treason, sedition, subversive activity, or disaffection is suspected because of the receipt or development of credible derogatory information. The primary purpose of each CTI is to produce information of such a nature, form, and reliability that the requesting agency (action agency) may determine the extent and nature of action, if any, necessary to insure the security of the Army.

9–2. Incident and Personal Subject Cases
Complaint-type investigations may be either incident or personal subject cases.

a. Incident Cases. Incident cases concern acts or activities which are committed by, or involve, an unknown person or group of persons. Examples of incident cases are—
   (1) Fire of suspicious origin in a sensitive military installation.
   (2) The theft of classified documents from a military office by person or persons unknown.
   (3) The distribution of subversive or seditious literature within a military installation by unknown persons.
   (4) Damage to equipment or supplies which is obviously manmade and malicious in nature.

b. Personal Subject Cases. Personal subject cases involve one or more known persons. Examples of activities or individuals which might result in the conduct of personal subject complaint investigations include—
   (1) Membership or affiliation with one or more subversive organizations by a member of the US Army.
   (2) Collaboration with the enemy, or misconduct as a prisoner, by a member of the US Army in prisoner-of-war status.
   (3) Negligent loss or failure to promptly report the loss of defense information by the military custodian of such information.

9–3. Complaint Type Case Categories
All complaint cases, whether incident or personal subject type, will be assigned a specific case category for control, reporting, and statistical purposes. (See AR 381–125, and AR 381–130 for explanation and definitions.) These categories are—
   a. Sabotage
   b. Espionage
   c. Treason
   d. Sedition
   e. Subversive activity
   f. Disaffection

9–4. Conduct and Control
   a. Instructions concerning the control and direction of complaint investigations are prescribed in AR 381–130 and AR 604–10.

   b. Investigation of cases which contain allegations that, if proved, would constitute offenses under civil or military law are conducted with a view toward developing information of sufficient probative value to permit its use in the appropriate civil or military court. However, such investigations should not be limited to the production of evidence, and the investigative reports should include all relevant and material information inadmissible in a civil or military court of law.

   c. The scope of knowledge and skills which the Special Agent must possess to successfully conduct CTIs encompasses all aspects of the techniques and procedures described in chapters 3 through 7. Special Agents assigned to conduct complaint-type investigations must also have a thorough understanding of the objectives and operations of hostile espionage, sabotage, and sub-
verse organizations (FM 30-17A). Extensive counterintelligence investigative experience is usually an essential requirement for Special Agents designated to conduct CTIs. Equally or greater in importance when conducting counterespionage operations is the need for an individual with training and/or experience in MOS 9668/972A/97C.

Section II. SABOTAGE INVESTIGATIONS

9–5. General

The essence of the crime of sabotage, Title 18, United States Code, chapter 105, sections 2151–2156, is the deliberate injury, destruction, or defective production of national defense or war materials by either an act of commission or omission. Because the first indication of sabotage normally will be the discovery of the injury, destruction, or defective production, most sabotage investigations will be incident type cases; i.e., cases involving an unknown person or persons. It can be anticipated that acts of sabotage, both in overseas areas-of-operation and in CONUS, will increase significantly in future wars, regardless of the type or level of conflict. Sabotage is a particularly effective weapon of guerrilla and partisan groups, operating against logistical and communications installations in occupied hostile areas, and of insurgents in internal defense operational areas. Acts of sabotage may be committed by trained saboteurs sponsored by hostile guerrilla, insurgent, or intelligence organizations; they may be conducted by individuals operating independently and motivated by revenge, hate, spite, or greed. In an internal defense or limited war situation where guerrilla forces are active, care must be taken to distinguish those acts involving clandestine enemy agents or dissatisfied friendly personnel from overt acts of war perpetrated by armed enemy units.

9–6. Types of Sabotage

Incidents of sabotage or suspected sabotage normally are classified according to the means employed. The traditional types of sabotage have been incendiary, explosive, and mechanical. In the future, it can be expected that chemical, biological, and nuclear means of sabotage will pose an even greater threat to military operations. A detailed discussion of materials and devices employed in these types of sabotage is included in FM 19–30. Special operations designed to counter the overall threat of sabotage to the military establishment are covered in FM 30–17A.

9–7. Investigative Procedure in Sabotage Investigations

Immediate action is of paramount importance in conducting a sabotage investigation. The possibility may exist that the saboteur is still near the scene, or that other military targets may require immediate additional security protection or preclude or limit further damage. Of vital significance is the preservation and analysis of the incident scene before the evidence may be altered or destroyed.

a. General Investigative Guidelines. The investigation must proceed with objective, analytical, logical thoroughness. The standard investigative interrogatives should be applied, usually in the following sequence:

(1) What. The Special Agent must determine what military target was sabotaged and the degree of damage to the target.

(2) When. The exact time when the act of sabotage was initiated and when it was discovered must be established and confirmed from as many sources as possible.

(3) Where. The precise location of the target and its relation to surrounding activities must be determined.

(4) How. The type of sabotage (incendiary, explosive, mechanical, biological, or nuclear) must be established and the procedures and materials employed determined through investigation and technical examination and analysis.

(5) Why. All possible motives of the saboteur may be established through a process of elimination by investigation of suspects determined to have had motive and opportunity to conduct the sabotage act.

b. Specific Investigation Actions. The following outline of possible investigative actions may be employed as a guide for investigation of most incidents in which sabotage is alleged or suspected:

(1) Obtain and analyze the details surrounding the reporting of the incident to the counterintelligence unit. The identity of the person report-
ing the incident and his reasons for doing so must be established. The facts connected with the reported discovery of the sabotage must be determined and examined for possible discrepancies.

(2) Examine the incident scene as quickly as possible. The Special Agent should attempt to reach the scene before possible witnesses have dispersed and evidence has been disturbed. Upon arrival at the scene, he should employ the standard crime-scene investigative procedures, to include the following steps:

(a) Protect the scene from mutilation by removing all unauthorized personnel from the area, roping off the area if necessary, and posting one or more guards to deny entrance and prevent anything from being removed.

(b) Locate all possible witnesses, record their names and addresses, and if feasible, hold them for questioning. Witnesses held should be segregated.

(c) Preserve the incident scene by taking notes, causing detailed sketches to be made, and taking pictures.

(d) Obtain the assistance of technical experts to search the scene of the sabotage act, collect and preserve physical evidence, and obtain all possible clues. Arson specialists, explosives experts, or other types of technicians may be required.

(e) Take any steps necessary to prevent further damage to the target and to safeguard classified information or material.

(3) Interview witnesses and attempt to obtain written statements before the witnesses have had a chance to forget details or compare stories.

(4) Based on facts determined from incident scene examination and interview of witnesses, check all pertinent files. Files of particular importance may include unit modus operandi files, partisan, guerrilla, or insurgent activity files, local police files on arsonists, local police modus operandi files, and Provost Marshal files. File checks should include personality checks on witnesses and the person who discovered and reported the act of sabotage.

(5) Interrogate suspects. All available information such as evidence, technical and laboratory reports, statements of witnesses, and information from informants should be compiled and studied in preparation for interrogation of suspects. In some instances, discreet surveillance may be employed prior to detention and interrogation of suspects.

c. Additional Aid. FM 19–20 contains investigative guidance particularly applicable to the investigation of incendiary sabotage; is a valuable aid in the conduct of complaint investigations in which explosive sabotage is alleged or suspected; and provides excellent guidance for the protection, search, and processing of the incident scene.

Section III. ESPIONAGE INVESTIGATIONS

9—8. General

Unlike sabotage cases, most espionage investigations will be personal subject rather than incident type cases; that is, they will originate with allegations regarding the activities of known individuals. There are instances, however, when counterintelligence investigations will be directed to conduct investigations of incidents in which espionage is suspected, but the identity of suspects has not been established (e.g., the theft of classified documents or materiel). Leads in espionage investigations may originate from a wide variety of sources, prominent among which are the following:

a. Reports from confidential sources.

b. Reports from other intelligence, security, and law enforcement agencies.

c. Discovery of evidence of espionage during surveys, inspections, and technical surveys or inspections.

d. Reports submitted by military units in accordance with provisions of AR 381–12 regarding espionage directed against the US Army and US Army personnel.

e. Discovery of evidence of espionage during screening of refugees, line crossers, displaced persons, prisoners of war, and similar groups.

f. Information developed during the course of routine personnel security investigations.

g. Information or evidence obtained through censorship operations.


The espionage statutes encompass many kinds of activities and have the ultimate goal to prevent defense information from falling into the hands
of a foreign nation. The salient aspects of the Federal Espionage Act, Title 18, United States Code, Sections 793-796, are summarized as follows:

Whoever for the purpose of obtaining information respecting the national defense—

a. With the intent or reason to believe that the information is to be used to the injury of the United States or to the advantage of a foreign nation:

(1) Goes into a place connected with the national defense, for the purpose of obtaining defense information, or—

(2) Copies anything connected with the national defense, or—

(3) With either lawful or unlawful possession, delivers national defense information to one not entitled to receive it, or fails to deliver on demand to one entitled to receive it, or—

(4) Receives or obtains any writing connected to the national defense with reason to believe that it was obtained contrary to law, or—

b. With intent to communicate to the enemy during time of war, collects, communicates, or attempts to elicit information pertaining to the public defense, or—

c. With lawful possession, permits national defense information to be lost, stolen, or abstracted; or having knowledge of such loss, theft, or abstraction fails to make a prompt report of the same will have committed espionage.

9—10. Investigative Guidelines in Espionage Cases

a. Analysis of the statute and of pertinent court decisions permit the following conclusions to be drawn with respect to proof of espionage.

(1) “National defense information” is information of military significance which has not been published for public consumption; i.e., not distributed in public channels. It need not be classified defense information as defined in AR 380-5. The critical points are that it relates to the national defense and has been restricted to authorized channels.

(2) “Any foreign nation” means the nation involved need not be a declared enemy, as in treason.

(3) Loss through gross neglect requires no positive act because it is a crime of omission.

Each facet, grossly negligent loss and failure to promptly report, is a separate and distinct crime.

b. The espionage investigation must be directed toward the collection of information and evidence to show—

(1) That national defense information was involved.

(2) That there was an intent or reason to believe that the United States would be injured, or that a foreign nation would benefit.

(3) That one or more of the acts enumerated in the statute actually occurred.

9—11. Spying, Article 106, Uniform Code of Military Justice

a. Although the crime of spying as defined in Article 106, UCMJ, differs from espionage, complaint-type investigations based on Article 106 will be categorized as espionage cases for reporting and statistical purposes.

b. Spying is strictly limited to a wartime military situation because of the requirements of international law, particularly the provision of the Geneva Conventions. There are four elements to the crime; all four must be present to constitute the crime of spying—

(1) Breach of our lines and apprehension within US zone-of-operations.

(2) Clandestine operations or false pretenses.

(3) Obtaining or seeking information to communicate to the enemy.

(4) Specific intent to so communicate.

9—12. Conduct of Espionage Investigations

Because of the wide variety of circumstances under which espionage cases may originate, the many different elements that may constitute the crime of espionage, and the fact that it may not always be desirable to direct the course of the investigation toward the arrest and prosecution of the offender, no single set of investigative procedures can be recommended as applicable to the conduct of espionage investigations. It is essential that Special Agents responsible for such an investigation have a thorough and up-to-date knowledge of all espionage and counterespionage methods and procedures discussed in FM 30-17A. Any or all of the investigative techniques described in this manual and FM 30-17A may be employed in espionage cases. Records examinations can be used to break the cover story of an
Section IV. TREASON INVESTIGATIONS

9-13. General

a. The abuse of treason statutes in English legal history led the framers of the US Constitution to include a limiting definition of treason in that document. The Constitution also imposes qualifications regarding the conviction of an individual for that crime—“no person shall be convicted of treason unless on the testimony of two witnesses to the same overt act, or on confession in open court.” (Article 3, US Constitution.)

b. Counterintelligence complaint-type investigations in which treason is alleged or suspected may occur during wartime, but are more apt to be directed immediately upon the conclusion of hostilities. 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. Treason cases will almost always be personal subject rather than incident cases. Unlike most other complaint type investigations, the investigation of a treason case will be primarily concerned with obtaining evidence of past rather than current activities of the suspected or accused person.

9-14. Elements of Treason Under Federal Statute

a. Interpretation by the Federal courts in treason cases leads to the following generalities concerning the legal elements of the crime of treason under the Federal statute:

(1) The accused must owe allegiance to the United States. A US citizen owes permanent allegiance whether in the United States or on foreign soil (unless an effective renunciation of citizenship was made). An alien in the United States owes temporary allegiance to the US because he enjoys the protection of US laws.

(2) A levy of war must be an actual waging of open hostilities against the Government with specific intent to cause its overthrow.

(3) Adherence to the enemy means, in general, any act committed after a state of warfare exists which indicates a want of loyalty to the Government of the US, and sympathy with its enemies, and which, by fair construction is directly in furtherance of their hostile designs.

(4) The levy of war and adherence to the enemy are alternative acts, either of which, when done by a person owing allegiance to the United States, constitutes treason.

b. The investigative burden in treason cases is as follows:

(1) Allegiance to the United States at the time of the act of treason must be shown.

(2) A levy of war under the two following conditions must be shown:
   (a) Open hostilities against the US Government must be shown.
   (b) Specific intent to overthrow the Government of the United States must be established.

(3) There must be an adherence to the enemy under these conditions:
   (a) Tangible or intangible aid to an enemy must be shown.
   (b) The enemy must be in a state of open hostility with the US Government.

(4) Two witnesses to the same overt act must testify or—

(5) It must be established that the accused intends to confess in open court.

Investigations conducted by counterintelligence personnel to prove or disprove charges brought against an individual subject to the UCMJ under Article 104, Aiding the Enemy, may in some cases by categorized as treason cases (AR 381–130). The article provides that “any person who (1) aids, or attempts to aid, the enemy with arms, ammunition, supplies, money, or other things or (2) without proper authority knowingly harbors or protects or gives intelligence to, or communicates, or corresponds with or holds any intercourse with the enemy, either directly or indirectly, shall suffer death or such other punishment as a court-martial or other military commission may direct.”

a. Physical Acts Which Constitute Aiding the Enemy. From the wording of the article and from interpretation by the Court of Military Appeals, there are three physical acts which constitute the crime of aiding the enemy. Any one of these acts with general criminal intent is a violation of the article—

(1) Aiding the enemy with ammunition, arms, supplies, or other things.
(2) Harboring or protecting the enemy without proper authority.
(3) Giving intelligence to, communicating with corresponding with, or holding any intercourse with the enemy without proper authority.

b. Proof Requirements Under Article 104.

(1) It is necessary to prove only that one or more of the prohibited acts actually occurred.
(2) The enemy need not be a declared enemy but may be a “substantial” enemy as in the case of the Communist forces in the Korean War or in the Vietnam conflict.
(3) The requirements of proving allegiance and proving the overt act by two witnesses which are essential under the Federal treason statute do not apply.

c. Korean War Cases Under Article 104. Article 104 was used in the majority of the courts-martial cases arising from the Korean prisoner of war incidents. Most of the specifications in these cases concerned the third act listed above and specifically that part of the act making correspondence, without proper authority, a crime. The Court of Military Appeals established in these cases that there are only three types of communication with the enemy which may be made with “proper authority” under military law, regardless of the motive which prompt the communication:

(1) A communication disclosing name, rank, SSN, and date of birth.
(2) A communication concerning the necessities of life.
(3) A communication concerning regulations and orders of the place of confinement.

9–16. Conduct of Treason Investigations

Records examination, interview, and interrogation normally will be the principal investigative techniques employed in treason complaint cases. The Special Agent must give particular attention to the legal requirements governing the collection and preservation of evidence, especially the taking of statements from witnesses and suspects. He must be careful to sort out fact from rumor or hearsay when taking testimony from witnesses and when reporting the results of investigations. In many cases, it will be necessary for the investigator to consult regularly with legal authorities during the course of the investigation to insure that the elements of proof are being fulfilled and that all applicable legal conditions and restrictions are met.

Section V. SEDITION INVESTIGATIONS

9–17. General

Complaint-type investigations regarding alleged or suspected sedition may be based on either the Federal sedition statute (Sections 2384 and 2385, Title 18, United States Code) or the UCMJ (Article 94, Mutiny and Sedition). Sedition cases may be either incident type, as in the case of the discovery of literature advocating the violent overthrow of the US Government, or personal subject type, as in the distribution of such literature by known persons. Leads or allegations which prompt the opening of sedition investigations by control offices may come from many sources, but they are most often based on information: submitted by confidential sources; contained in reports from other agencies; or developed during the course of routine background investigations. Complaint-type investigations in-
volving sedition may occur with equal frequency in either peacetime or periods of hostilities.

9-18. Seditious Conspiracy
Section 2384 of Title 18, US Code, makes it a specific crime to conspire to overthrow the Government of the United States. 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 toward fulfillment of the conspiracy's objective. 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 United States. It should be noted that seditious conspiracy is a conspiracy to actually overthrow, as distinct from a conspiracy to advocate overthrow.

9-19. Advocacy of the Overthrow of the US Government
Section 2385 of Title 18, US Code, also known as the Smith Act, enumerates four specific types of activity which, if done with intent to cause the overthrow of the Government by force or violence, constitute seditious conspiracy. The prohibited acts are: advocating or teaching the duty or necessity of such overthrow; or printing, publishing, selling, or distributing written matter advocating or teaching the duty or necessity of such overthrow; or organizing a society or group whose purpose is to advocate or teach the duty or necessity of such overthrow; or being or becoming a member of, or affiliating with, such society or group knowing the purpose thereof. Court decisions relative to 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 of forcible overthrow of government as an abstract principle, divorced from any effort to instigate action to that end, does not constitute the crime of sedition under the Smith Act. The requirement for the advocacy to "incite persons to take action" is of particular significance to the Special Agent, and it can be expected that considerable effort in any case alleging violation of the Smith Act will necessarily be directed toward proving that the oral or written material involved intended to incite listeners or readers to take action.

Counterintelligence personnel may be directed to investigate sedition or (less frequently) mutiny cases. Such complaint-type case may be either personal subject or incident type.

a. Mutiny. Mutiny is defined as a collective effort to overthrow lawful military authority. It also includes, under Article 94, the individual creation of a riot or disturbance with the intent to overthrow lawful military authority. The offenses may be committed in two ways: by several persons acting in concert to refuse to obey orders from proper authority, and with intent to override military authority; or by a person, with similar intent, acting either alone or in concert with others, creating a violence or disturbance. The investigation of incidents of mutiny normally will not be assigned to counterintelligence personnel unless the mutiny is believed to be related to hostile intelligence or subversive activities.

b. Sedition. Article 94 makes it a crime for any person, with intent, to cause the overthrow or destruction of lawful civil authority, or to create in concert with any other person a revolt, violence, or other disturbance against such authority. The investigation of charges of sedition under Article 94 normally will be assigned to counterintelligence personnel.

Covert investigative techniques are likely to be applicable to the conduct of sedition investigations. The standard techniques of interview and interrogation will also be important. A thorough knowledge of subversive activities, individuals, and organizations in the area usually will be an essential attribute for Special Agents conducting sedition complaint cases. FM 30–17A provides additional investigative techniques likely to be applicable to the conduct of sedition investigations.
verse loyalty information developed during routine background investigations; reports submitted by military units under AR 381-12, reports from other intelligence and security agencies; and leads obtained directly from sources used in counterintelligence special operations (AR 381-47 and FM 30-17A). Because neither subversive activity nor disaffection, as such, is defined as a specific crime in either the Federal criminal code or the UCMJ, the objective of such complaint-type investigations usually will be to determine if there is a need for some administrative action; e.g., removal from the sensitive assignment to protect the security of the military command.

9–23. Subversive Activity
AR 381-130 defines subversive activity as all willful acts which do not fit the categories of sabotage, espionage, treason, or sedition, but which are intended to lend aid, comfort, or moral support to individuals, groups, or organizations advocating the overthrow of the United States Government by force or violence, or are otherwise intended to be detrimental to the national security of the United States. Since this area is very nebulous and there are no statutory standards which the actor's conduct must meet, the investigation must:

a. Determine what act occurred,

b. Show, based on evidence of probative value, that the activity was detrimental to the national security, and

c. Show that the activity did not rise to the level of treason, sedition, espionage, or sabotage.

AR 604-10 and AR 690-1 include specific guidance regarding the conduct of complaint-type investigation of alleged subversive activities on the part of uniformed or civilian personnel of the Department of the Army.

9–24. Disaffection
Disaffection, as defined in AR 381-130, is a state of mind and, although the disaffected person may have criminal intent, there is no conduct involved. Hence, disaffection is noncriminal in nature. However, a person within the military establishment possessing such a state of mind creates a vulnerable spot in the national security and is most susceptible to approach by persons whose objectives are inimical to the United States. The Special Agent must show the requisite mental attitude for disaffection through such tangible indications as oral statements, written statements in personal correspondence, published statements, or published textual material.
CHAPTER 10
COUNTERINTELLIGENCE SURVEYS AND INSPECTIONS

Section I. COUNTERINTELLIGENCE SURVEYS

10–1. General

a. One of the functions of counterintelligence units is to assist commanders in establishing systems, procedures, and safeguards designed to protect military installations, personnel, and activities from the threat of espionage, sabotage, and subversion. To determine the requirements for establishing such systems, procedures, and safeguards, it is necessary: to analyze all counterintelligence factors influencing security at the commander’s installation; to ascertain the counterintelligence measures required by the sensitivity or criticality of the installation; to determine the counterintelligence measures which now exist, and finally; to provide recommendations which will bring existing counterintelligence measures to the required standards. The accomplishment of these four requirements is the objective of the counterintelligence survey.

b. The counterintelligence survey is a service to determine the security measures necessary to protect military installations and offices against espionage, sabotage, and unauthorized disclosure of, or access to, classified defense information. While Army Regulations provide certain minimum requirements for security, and inspections are made to determine that these requirements are being met, the scope of the counterintelligence survey is much broader, as it must provide recommendations designed to fit a specific installation. Because the survey is to establish requirements rather than test compliance with established requirements, it is not a recurring service. As long as there is no major change in the physical characteristics of an installation or its mission, the counterintelligence survey once conducted will remain valid.

c. Physical security is a responsibility of the Provost Marshal (AR 190–13). However, in accordance with Department of the Army policy, personnel performing CI services are responsible for assessing the CI aspects of security plans and programs. Counterintelligence surveys are coordinated with the local provost marshal who, under the staff supervision of the G1, develops and executes plans and procedures pertaining to crime prevention, maintenance of discipline, law, order, and physical security.

d. Signal security is the responsibility of the US Army Security Agency (USASA). USASA elements monitor and analyze Army telecommunications and evaluate the status of communications security (COMSEC) in support commands. Additionally, these elements assist in determining the electronic security (ELSEC) characteristics of Army equipment systems and recommend operating techniques and procedures for ELSEC purposes. See FM 32–5 for details on USASA assistance to CI elements.

10–2. Initiation of a Counterintelligence Survey

The request for a CI survey must originate with the commander of the installation concerned or with a higher commander in the same chain of command. A CI survey may be requested for the following reasons:

a. Activation or reactivation of an installation or activity, or a major component thereof.

b. Significant change in mission, function, personnel strength or structure, or physical reorganization.

c. New, hazardous conditions within an installation which necessitate the re-evaluation of the security system.

d. Significant change in material produced, processed, stored, or handled.

e. Change in the locale or environment in which the installation is located.

f. Receipt of sufficient justification for reasons other than those stated above, such as no record of a previous survey having been conducted.
Section II. PREPARATION FOR COUNTERINTELLIGENCE SURVEYS

10—3. Preparatory Procedures

a. Selection of Personnel. The number of personnel used to conduct the survey will vary according to the size and nature of the installation, the number of personnel available, and special operational or technical considerations. In some cases, the survey may be conducted by a single Special Agent; more often it will be conducted by a team operating under the direct control of a designated Special Agent-in-Charge. Frequently, the team will include personnel who have been trained in defense against methods of entry (DAME), audio surveillance countermeasures (DASE), and investigative photography (Photo).

b. Collection of Data. It is essential that the survey team be as well informed as possible relative to the particular installation to be surveyed. Counterintelligence unit files, particularly records of prior surveys or inspections, will provide valuable background and reference data. Information regarding the area surrounding the installation to be surveyed may be found in investigative or other intelligence reports in unit files of the military intelligence element, the Provost Marshal's Office, and the local Criminal Investigation Command (CIDC) element. In particular, the CIDC Crime Prevention Surveys, both external and internal, will assist the survey team in the conduct of the survey. Other investigative or intelligence agencies in the area may also be able to assist, e.g., OSI and NIS. Additional information relative to the geography of the area can be obtained from road or military maps. Regulations and directives pertinent to the installation to be surveyed, if available, should also be collected and studied.


d. Equipment. The survey teams should procure tools and equipment which will be needed during the conduct of the survey. Such items may include tools (hammer, screwdriver, sidecut pliers, measuring tape, small crowbar, flashlight), photographic equipment, special technical devices, and appropriate office equipment for preparing records and reports.

e. Coordination. A designated representative of the counterintelligence unit concerned normally will contact the commander of the installation/activity to be surveyed prior to the initiation of the survey for the purposes of:

(1) Determining and coordinating the proposed scope of the survey.

(2) Arranging for access to necessary records, buildings, and areas.

(3) Procuring applicable installations/activity security directives.

(4) Arranging for an initial briefing prior to the actual conduct of the survey, at which time the Special Agent-in-Charge of the team will thoroughly brief key installation personnel on what is to be accomplished and answer any questions concerning the survey that they may have.

10—4. Preparation of Checklists

a. Study and analysis of data collected regarding the installation to be surveyed may indicate the necessity or desirability of preparing a checklist to serve as a guide for personnel conducting the survey. A checklist is a list of general or specific points that must be covered during the survey. It serves as a reminder to surveying personnel to insure that the scope of the survey is met. A checklist may be either general or specific.

(1) General checklist. A general checklist provides reminders of the security considerations which are usually inherent to all installations; e.g., documents and information security, personnel security, and physical measures. Within these three major divisions, there will be many subdivisions.

(a) Documents and information security considerations may include storage facilities, marking and handling of classified documents, application of “need-to-know,” duties of security control personnel, maintenance of classified document log, and destruction procedures.

(b) Personnel security requires attention be given to clearance procedures, security education program, and similar matters.

(c) Physical measures include perimeter fencing, perimeter lighting, guard systems, pass and badge systems, restricted areas, and building security. In this connection, particular attention
is invited to the physical security checklist contained in FM 19-30. (Physical measures should be included in the physical security conducted by military police units under the control of the provost marshal.)

(2) Specific checklist. A specific checklist is one that applies to a particular installation or a unique type of installation. An example would be a checklist prepared for use at US Army Air Defense Command installations. In many respects, all of these installations are alike. Usually, these sites occupy the same amount of real estate, operate at the same echelon of command, have the same equipment, the same number and type of troops, and, in most cases, operate under the same policy from an operational and security point of view. When there is a requirement to survey a number of these installations, it would be worthwhile to prepare a specific checklist which would apply to these sites. Specific checklists normally include more detail than general checklists.

b. A checklist, either general or specific, is used only as a guide. It is improper to assume that any checklist will provide a complete basis for action in completing the survey. Each installation has its own particular security problems. These differences may have their origin in size, location, mission, or surrounding area of the installation. Each checklist must be modified by additions, changes, or deletions before it can be applied to any one installation. Even then, the application of good investigative techniques can be expected to extend the survey beyond the detail contained in the checklist. See appendix D for a checklist which may be used as a guide for conducting a CI survey.

10-5. The Escort Officer

a. From the standpoint of both the Special Agent team and the installation, it is desirable that an escort be provided by the installation to accompany the survey personnel during the conduct of the survey. Preferably, this escort should be a representative of the installation's intelligence or security office. In any event, he should be a person conversant with all security practices and procedures in effect at the installation.

b. The escort officer serves as a guide to the Special Agent or survey team as they proceed through the installation conducting the survey. He identifies the surveying personnel to those persons who will give information and makes arrangements to satisfy their operational requirements. The escort officer is present to gain timely notice of any outstanding hazards discovered, provide information pertaining to previous attempts to correct such hazards, and make such on-the-spot corrections as possible.

Section III. CONDUCT OF COUNTERINTELLIGENCE SURVEYS

10-6. Preliminary Exterior and Interior Checks

As soon after the initial briefing as possible, the survey team should conduct a tour of the area surrounding the installation. The purpose of such an inspection is to gain a general knowledge of those elements outside the installation which do or could conceivably have a direct or indirect influence upon the security of the installation either in peacetime, under actual war conditions, or in case of riot, strikes, or other domestic disorders. It is in these areas adjacent to the installation that many of the installation personnel gather for relaxation or entertainment, often under circumstances conducive to "loose talk." The survey team should also check geographical features: terrain, road and railroad networks, bridges, and natural or manmade hazards near the installation. They should also determine, to the greatest extent possible, what influence the population has or could have upon the security of the installation. The CIDC Crime Prevention Survey (External) may assist greatly in this area. The team should also tour the interior of the installation to determine those areas, buildings, or offices which will require additional security considerations or which are considered to be sensitive. After the inspection, it may be necessary to confirm the findings by arranging for an interview with staff officers of the installation to learn the operational importance of particular areas of buildings.

10-7. History of the Organization and Installation

When survey personnel have completed a check of the surrounding area of the installation and a preliminary survey of the interior of the installation, they should be ready to commence the actual survey. The team should first determine the his-
tory of the organization to be surveyed and of the
installation on which it is located. In most cases,
the history, background information, or both are
readily available in printed form. From a secur-
ity point of view, the survey personnel are inter-
ested in the history of the organization and in-
stallation from its inception. There frequently is
information in the history of the organization or
installation which directly affects the current se-
curity situation (abandoned tunnels or sewer
lines).

10-8. Establishment of the Installation’s
Sensitivity

At this point, the security needs of the installa-
tion in relation to its sensitivity and importance
must be determined. During the preliminary sur-
vey the survey team has had an opportunity to
make a rough evaluation of the installation’s im-
portance to national defense and its vulnerability
or value as an espionage or sabotage target. An
accurate appraisal must be made prior to the in-
vestigation in order that specific recommenda-
tions commensurate with the actual security
needs of the installation can be presented to the
commander and his staff. The following points
should be considered in determining sensitivity:

a. Mission. The first consideration is the mis-
sion of the organization being surveyed. It must
be determined if the mission is continuous or of
short duration, unclassified or classified, and if
technical or highly skilled personnel are neces-
sary for its successful operation.

b. Cost of Replacement. In estimating the cost
of replacement of the installation, a comparative
analysis, not a dollar and cents figure, is ob-
tained. The time necessary to replace personnel,
documents, and materiel in the event the installa-
tion were neutralized or destroyed is estimated.
Further consideration is given to potential
sources of personnel of similar experience and
knowledge and to a source of copies of essential
and critical documents which would be required
in replacing or reactivating the installation. The
financial cost of replacing the installation may
then be considered.

c. Location. Consideration must be given to the
location of the installation and the effect the ele-
ments surrounding it have upon its security. Most
of the information concerning this aspect is de-
termined from file checks and examination of the
surrounding area before actually commencing the
investigation. The area may be highly industrial,
congested residential, urban in nature, or
sparsely populated. The type of surrounding area
may offer favorable natural cover to enemy es-
ionage or sabotage agents. Consideration should
also be given to the area’s transportation facili-
ties and to natural hazards which may arise from
the surrounding area such as flood, forest fires, or
adjacent flammable storage areas.

d. Security Classification of Information. One
of the major points for consideration in evaluat-
ing the sensitivity of an installation is the classifi-
cation of the information stored, used, and
created there. Logically, information which is of
greater importance to national defense required
greater safeguarding from all standpoints. While
Army Regulations establish some safeguarding
requirements, comparable measures will very
likely be required in areas of consideration not
specifically established by regulations. When con-
sidering the classification of information, the
amount of classified information present must be
determined.

e. Number of Like Installations. In determin-
ing the overall importance of an installation, con-
sideration must be given to installations or activi-
ties which are capable of absorbing the functions
of the surveyed installation in order to maintain
mission continuity, in the event the surveyed in-
stallation were neutralized or destroyed. If no
other organization is capable of assuming these
duties, the importance of the surveyed installa-
tion would be increased immeasurably. However,
the mere fact that similar installations or activi-
ties exist may not significantly lower the critical
rating. Similar installations may be in no position
to absorb the mission of another, or, if the mis-
sion is primarily devoted to a defined geographi-
cal area, there may be no substitution regardless
of how many similar installations exist. In con-
sidering the substitution or replacement of an in-
stallation or its mission, due consideration must
be given to the time factor. What will be the time
consumed before the changeover or substitution is
effected? Are the facilities of the alternate in-
stallation of such a nature as to achieve an oper-
ating efficiency comparable to the previous level?
If the alternate installation cannot operate at an
acceptable level of efficiency, how long would it
take to attain this desired level. Will this transi-
tion period affect the national defense effort to a
great degree? All of these questions must be con-
sidered concerning the number and adaptability
of like installations.
f. Importance to the Defense Effort. In some instances, evaluation of the installations importance may be made locally based upon a joint effort between the CI survey team, the installation commander, and his staff. Other knowledgeable persons within the installation and command and an evaluation and correlation of available information from other agencies, adjacent commands, and the agency utilizing the end product are also of prime importance. In most instances this evaluation has been made at higher echelons of command or at Department of the Army level. The basic consideration is how important is this installation and its mission, functions, and production to the national defense effort. The mission of the installation affords a fairly good indication of its importance. However, when the mission is compared with the cost of replacement, location of the installation, existence of like installations which could absorb the operations, and classification of the installation's activities and information, the overall importance of the surveyed installation may be higher or lower than anticipated. This is the information the survey team requires before it can determine the actual security needs of the particular installation. When this sensitivity rating is compared with the installation's current security situation, the investigator will be in a position to offer recommendations to either raise or lower the level of security on the installation in consonance with its sensitivity or importance to the national defense effort.

10-9. Determination of Existing Security Measures

a. The foundation having been laid, the survey personnel can devote themselves to examination of the existing security situation at the installation. This portion of the survey is a minute examination of all factors pertaining to personnel security, physical measures, and document and information security. It is a collection of factual data that will, when reported, show what exists at this installation that affects security, without regard for its being labeled as a hazard or a precaution. Much of the security situation will not be based upon existing written requirements. Therefore, much of what is examined will not have been officially determined to be hazardous or precautionary in nature. The survey team must arrive at its own conclusions that these factors will be reflected in its recommendations.

b. The techniques of conducting this portion of the survey are dependent upon the number of survey personnel available, personnel capability, and choice. Since three types of security are involved (document and information, personnel, and physical) and will be reported in separate portions of the survey report, it may be easier but more time-consuming to attack each of the types as a separate problem (i.e., gather all the information pertaining to physical measures first and then return over the same ground gathering information pertaining to personnel security). If more than one Special Agent is available, it is better for a two-man team to investigate jointly than to use individuals in separate areas. If sub-teams of two or more investigators are assigned to separate portions of the survey to facilitate its accomplishment, extensive coordination is required during the information-gathering portion and the evaluation portion because of the interaction between the types of security or areas being considered.

10-10. Document and Information Security

The document and information security phase is probably the most important part of the CI survey. Accordingly, this portion of the survey must be minutely detailed. In addition to using a checklist, survey personnel must examine, analyze, check and cross-check always seeking to correct weaknesses and discrepancies. Each survey team member must visualize the security procedures employed from a viewpoint of an enemy agent. Many aspects of document and information security appear to be mechanical in nature, but these appearances are misleading. Security, in all its phases, must be an alert, live process in order to constitute an effective defense against enemy agents attempting to penetrate or destroy the installation. With these ideas in mind, the survey team can effectively inspect the procedures used, evaluate the security situation, and recommend to the commander corrective measures necessary to eliminate weaknesses and gaps in existing procedures. Conduct of the survey of document and information security will include consideration of the following specific areas:

a. Organizational Structure. The survey team must first have a clear understanding of the organizational structure of the installation or unit being surveyed in order to check the security and flow of classified information. This can best be determined by interviewing individuals who likely have a thorough knowledge of the structure and operational relationship between the installation and the units stationed thereon. Organ-
izational charts obtained from the facility and units to be surveyed are also of great assistance in this respect.

b. Flow of Classified Documents. The inflow of classified information generally commences at the higher headquarters and continues down through intermediate offices to lower units. The outflow of classified information usually follows the reverse pattern. The suggested approach is to examine all applicable items at each message center or classified document control or storage point before proceeding on to the next point to be checked.

c. Document Records. Classified document registers, receipts, retirement records, and destruction certificates are accounting records. They are part of a protective system designed to overcome human error by assisting individuals to systematically handle classified information in a secure manner. Accountability records are also detective in nature, for discrepancies may indicate loss, theft, or possible compromise of the information. Such records may also indicate by their accuracy and completeness, the attitude of the individuals administering the records toward security.

10–11. Personnel Security

Personnel security, from the viewpoint of the conduct of a CI survey, may be divided into two separate categories, security clearances and security education. The security clearance program is discussed below; security education is covered separately in paragraphs 10–19 through 10–22.

a. Security Clearance Program. The personnel clearance procedures for an installation or unit must be carefully audited. AR 380–5 established that the basic requirement for dissemination of classified information is a “proper clearance” and a “need-to-know.” A proper clearance is obtainable only upon initiation of appropriate administrative action by the command in accordance with AR 604–5. The system for initiating a request to a higher headquarters, to include all administrative measures and forms, should be carefully reviewed. Internal methods for supervision of preparation of requests, suspense files, tracers, and verifications of clearance status of incoming personnel should be clearly outlined in the installation or unit SOP. In those cases where the activities of a unit with a tactical capability are being surveyed, careful attention must be given to the security portion of the tactical SOP. A personnel security program under tactical conditions must be designed to insure maximum protection for classified information while insuring flexibility of command that is vital to successful combat operations.

b. Records on Security Clearances. The clearance level required by each TOE or TD position must be determined; this information should appear on a roster or manning table used by all staff sections for planning purposes. A comparison of the actual clearance level of personnel assigned and the clearance required by the position occupied will indicate the effectiveness of the program being surveyed. Each unit or installation should maintain a file on each individual assigned to the command to include forms executed and correspondence received or forwarded in connection with the personnel security clearance program (AR 340–18-series). A reference card file indicating the full name, date and place of birth, social security number, and duty assignment of all personnel possessing a security clearance should be maintained in the intelligence office. The system employed to insure the accurate and up-to-date status of the card file should be checked by the survey team.

(1) The distinction between the clearance level of an individual and the level of access to classified information authorized should be made clear. Surveying personnel should emphasize that a person may possess a Top Secret clearance, but in applying the “need-to-know” principle, a commander may limit access to that level of classified information consistent with the duty assignment of the individual.

(2) General efficiency of the personnel security program in the overall operation of the command is often indicated in the personnel assignment section. Each set of orders prepared on an individual should, whenever necessary, indicate the clearance status of the person concerned. A duplicate of the card file system in the intelligence office may be maintained in the personnel assignment section. If so, the administrative procedures practiced to insure that the duplicate set is always current should be examined by surveying personnel.

(3) Military personnel who have been cleared should have a valid DA Form 873 (Certificate of Clearance and/or Security Determination under EO 10450) in their 201 files. The clearance certificate of a civilian employee is filed in his official personnel folder. A signed copy of DD Form 98, (Armed Forces Security Questionnaire) for military personnel and DA Form 1111, (Statement of Nonaffiliation with Certain Organ-
izations) for civilian personnel must be a part of the permanent records of all military and civilian personnel of the Department of the Army. The DA Form 66 (Officer Qualification Record) and the DA Form 2Q (Enlisted Qualification Record) must indicate the date of completion of the investigations, type investigation and level of security clearance granted.

10–12. Physical Security

a. Physical security is understood to be a distinct type of security differentiated from document and information security and personnel security in that it comprises a system of controls, barriers, and other devices and procedures to prevent destruction, damage, and unauthorized access to Army facilities/activities. Counterintelligence surveys, conducted to assess the counterintelligence effectiveness of physical security plans and procedures, is not understood to include primary staff interest of the provost marshal in physical security surveys as described and defined in FM 19-20 and FM 19-30.

b. In the event the installation/activity being surveyed already has on record a physical security survey performed by military police personnel, a statement referring to the report is deemed sufficient, providing those deficiencies noted which directly affect the security of classified documents and material have been corrected. If this has not been accomplished, appropriate recommendations will be made in the written report.

c. If there is no record of a previously conducted physical security survey, coordination with the local provost marshal will be conducted in order to coordinate and schedule a physical security survey to be accomplished in conjunction with the CI survey. Counterintelligence personnel must, nevertheless, be familiar with, and prepared to examine and assess the counterintelligence effectiveness of, barriers, controls, and other protective devices, as well as the physical security plans and procedures of the installation concerned. When the facility being surveyed is of the “open post” type with few physical restrictions which relate directly to counterintelligence security requirements, emphasis will be placed on examination of physical security factors which directly affect classified storage areas, restricted areas, or sensitive locations. When the entire installation’s physical security system is essential to the protection of classified documents or material, the survey must be expanded to include these additional physical security safeguards.

d. Counterintelligence surveys and inspections by CI units, and SIGSEC surveys conducted by USASA units complement each other. Coordination through G2/S2 channels of these efforts serve to maximize the overall security posture of the installation.

10–13. The Exit Briefing

After the survey team has completed its investigation and has arranged the results of its work in draft form prior to departing the installation, it should determine if the commander and his staff desire a final conference or exit briefing. The Special Agent-in-Charge should discuss with the commander and any other individuals designated by the commander the findings and tentative recommendations. The recommendations are based on facts developed during the survey and cover the safeguards which should be established to adequately protect the installation against espionage, sabotage, and subversion. The recommendations should be tempered with reason, taking into consideration cost, time, manpower, availability of materials, etc. For each item which the survey team establishes as a hazard, there must be a reasonable, practical recommendation. A successful final critique with the commander and his staff can, in most cases, insure that the survey team’s recommendations are realistic and can be implemented with minimum difficulty. The team is not limited to the number of recommendations which can be made to eliminate any one hazard. Primary and alternative recommendations can be made to insure correction of the hazard by the alternative means if the primary recommendation cannot be implemented.

Section IV. COUNTERINTELLIGENCE INSPECTIONS

10–14. General

A CI inspection is a service performed to determine compliance with established security policies and procedures. In addition to the formal inspections discussed in this section, counterintelligence elements should maintain regular contact with all US Army units in their area in order to provide continuous informal assistance, support, and advice to commanders at all echelons regarding security.
a. The inspection, although akin to the survey, is much more restricted in scope, because the survey considers everything pertaining to security at an installation, while the inspection is limited to an assessment of the degree of compliance with established policies and procedures.

b. The preliminary and investigative procedures involved in the conduct of a CI inspection are essentially the same as those required for a survey. The selection of investigative personnel, necessary file checks and other preparation, duties of the Special Agent-in-Charge, use of checklists, coordination with the commander and escort officer, and actual inspection will very closely parallel the procedures used in the conduct of a CI survey. The usual differences between the procedures followed are a matter of degree. There may or may not be prior personal contact between the installation to be inspected and the counterintelligence unit. Often, the initial contact is made by a letter of notification originated by the headquarters to which the surveying unit is attached. The file checks need not be as extensive as those required for a survey because the field-of-interest is limited to an appraisal of the degree of compliance with established security policies and procedures. Normally, the conduct of the inspection will not include the history, mission, or establishment of installation sensitivity.

10—15. Scope
The scope of the CI inspection will include checks to determine the degree of compliance by personnel of the installation or activity with established security policies and procedures. Areas covered will include: whether assigned personnel with access to classified information and material are properly cleared; whether they are properly safeguarding classified information and material; facilities used for storing classified information and material to determine their adequacy; procedures which are practices in controlling entrances and exits; guard system; and guard personnel with reference to their instructions concerning security. Special emphasis will be placed upon findings noted during previous surveys or inspections to determine if corrective actions have been taken.

c. Announced Inspections. An announced inspection is one which has been publicized to the installation to be inspected so that all concerned personnel should be aware of its imminence and, consequently, may make such preparations as are necessary. This type of inspection is conducted on a recurring basis so that the installation, by making periodic preparations for forthcoming inspections, brings its security application to a high level and maintains a responsible level of security between the inspections. Announced inspections are often conducted in conjunction with annual inspections conducted by the Inspector General. Assistance may range from providing the installation with checklists which will be used in conducting the inspection to conferences with the installation's security personnel.

b. Unannounced Inspections. An unannounced inspection is known in advance to certain selected personnel only. This type of inspection is designed to determine the installation's compliance with existing requirements at times when special preparations have not been made. Personnel conducting an unannounced inspection must have with them, in addition to their credentials, authorization to accomplish the inspection. It is also necessary that they be accompanied by a responsible person of the command being inspected.

c. Penetration Inspections. A penetration inspection is conducted in such a way that installation personnel, other than the commander and those persons he feels it is desirable to notify, are unaware that such action is taking place. This type of inspection may be all-inclusive or may be limited to an attempt by counterintelligence personnel to fraudulently gain access to some sensitive area within an installation for the purpose of performing simulated espionage or sabotage acts. The simulated activities should correspond to activities which actually might be attempted by a foreign power or hostile agent, and be realistic. Penetration inspections should be planned and executed in a manner that will not impair or disrupt the activities of the inspected unit or installation unless this is within the context of the request and has been approved by higher headquarters.
Section V. REPORTS OF COUNTERINTELLIGENCE SURVEYS AND INSPECTIONS

10–17. General

a. The results of CI surveys and inspections will be recorded and forwarded by letter of transmittal to the requester. Normally, reports of CI services will contain five sections:

(1) I. Introduction
(2) II. Scope
(3) III. Findings and Recommendations
(4) IV. Comments
(5) V. Exit Briefing

b. Subparagraphs will be used within each section, as appropriate, and numbered consecutively throughout the report. Sketches, photographs, documents, or other pertinent material will be included when appropriate for clarity and understanding. Inclosures will be referred to and prepared as exhibits. Reports will be classified, marked FOR OFFICIAL USE ONLY, or unclassified according to content. Reclassification instructions or dates for removal of protective markings will be in accordance with AR 340–11, AR 380–6, and AR 381–45.

10–18. Preparation

Appendix C contains an example of a report of Counterintelligence Survey which should be used as a guide. The following provide additional guidance to assist the Special Agent in those items of interest to be included in Counterintelligence Survey and Inspection reports:

a. Section III. Findings and Recommendations.

(1) Findings. All violations, discrepancies, or deficiencies will be listed as findings, and all entries, will be sufficiently descriptive to convey a complete understanding to the serviced command. Each finding will be followed by an appropriate recommendation (see example in app C). Findings of a serious nature should be immediately brought to the attention of the appropriate official. Minor findings which are actually corrected in the presence of the inspection team or prior to their departure will be recorded with a statement to the effect that immediate corrective action was taken and therefore no recommendation is made.

(2) Recommendations. Recommendations should be concise, to the point, factual, and realistic. In many instances, a specific recommendation may require more than a partial quotation from published directives or regulations to adequately assist the command. Each recommendation should be phrased to eliminate both the basic problem and the underlying cause and should be followed by a specific paragraph reference to an applicable regulation or directive.

b. Section IV. Comments. Those existing conditions and procedures, which, although not in violation of or at variance with published regulations or directives, may possibly have an adverse effect on overall security, will be recorded as weaknesses. Any other matter of pertinency not recorded elsewhere in the report may be included. If there are no pertinent remarks or weaknesses noted, this should be indicated.

c. Section V. Exit Briefing. All findings and recommendations should be discussed with the key personnel of the serviced unit. Complimentary comments or discussion of substandard aspects of the security program should also be presented. The briefing will be made a matter of record in the closing paragraph of the report; the report will include the names and titles of all individuals present.

Section VI. SECURITY EDUCATION

10–19. General

a. Either in conjunction with the conduct of CI surveys and inspections or in the capacity of technical advisors on military security, counterintelligence personnel may assist commanders in planning and implementing security education programs. The assistance rendered may be advisory in nature or be an actual presentation of a portion of the education and indoctrination program. Assistance by counterintelligence personnel may be particularly helpful in conducting security orientations in accordance with AR 381–12, and AR 381–14.

b. Protection of classified information is the objective of security education, with an intermediate goal of security awareness on the part of all
personnel. The security indoctrination of an individual can be successful only when he consciously accepts security as his personal responsibility. Security consciousness is a state of mind implying an understanding of security objectives, principles and measures, and denoting a willingness and desire on the part of the individual to reach these objectives.

10–20. Planning a Security Education Program

In planning a security education program for a command, many factors must be taken into consideration for the program to be successful. The security requirements of commands will vary, as will the role of the counterintelligence unit in assisting the command in establishing a security education program. If the unit has been requested to suggest a security education program for a particular command, a preliminary appraisal is mandatory. Scheduled meetings with the commander, his staff, and key personnel will aid the unit in planning an effective program. Planning considerations include the following:

a. Mission. The mission of the command will usually indicate potential targets for hostile acts of sabotage, espionage, or subversion. The mission should be studied carefully to insure that the recommendations for a security education program are realistic, pertinent, and in harmony with the mission.

b. Standing Operating Procedures. All SOPs, including personnel security, document and information security, and physical security, must be examined to ascertain what security measures are in effect. After the review of these procedures, interviews with members of the command should provide a reliable means of assessing the degree of compliance with these established procedures. The interviewees should remain anonymous in order to encourage full participation. Personnel should be observed performing their duties to determine whether they are complying with the established security procedures.

c. File Checks. A perusal of the counterintelligence unit's files as well as those of allied federal or civil investigative agencies must be made to determine if any special security factors or hazards are to be considered.

d. Status of Security Training. During the preliminary appraisal, the status of the command's security training must be established. Not all personnel will have received the same amount or type of security training. Since their requirements vary, it will be necessary, for training purposes, to divide personnel into various groups: clerks and stenographers, custodial personnel, staff members, security forces, and operational groups. In establishing the status of security training within a command, the general attitude of all personnel toward this training and security in general should also be established. Care must be taken to insure that the attitude of the command toward security is not the opinion of key personnel alone. A cross-sectional survey of the entire command must be obtained in order to recommend an effective program.

ee. Survey of Surrounding Areas. A survey of the area surrounding the command should be made to establish the location and type of recreational facilities frequented by members of the command during off-duty hours.

10–21. Phases of a Security Education Program

A security education program should be cycled and suited to the requirements of a particular group. The number of phases required is dependent upon the number of people concerned, status of training, amount of time available, physical facilities available, and funds allocated the command for security purposes. Whenever practicable, elements of this program, particularly the initial interview and debriefing (a and g below), will be incorporated in unit SOP. In addition to the time spent in the actual education of personnel, a complete and balanced security education program must also include indirect methods of approach which will require additional utilization of supervisory and security personnel.

a. Initial Interview. The first phase of a complete and appropriately cycled security education program is the initial interview. The initial interview is usually the first contact that new members of the command will have with security, and it is imperative that the approach to this interview be conducted in a serious and professional manner. The interview may be supplemented by issuance of security regulations and written directives. The initial interview is designed to accomplish four purposes:

1. Impress the individual with the significance and value of the information with which he will be entrusted.

2. Stress the importance of security to the command, the US Army, and to the individual himself.
(3) Explain to the individual the penalties involved if he carelessly or negligently mishandles the information with which he has been entrusted.

(4) Insure that the individual fully understands that once he has had access to, and knowledge of, classified information, he assumes, at the time of receipt of this information, the responsibility for its safeguarding.

b. Training Conference. The second phase of a security education program is the training conference or conferences. The length of time involved depends on the complexity of security requirements pertaining to the individual's particular duties. The training conference should be held during the normal training or orientation period for new members of the command. It should be an integral part of training to emphasize that security is one of the important requirements and conditions of employment. Individuals should be grouped together according to their positions within the command and each group should be treated accordingly. During these conferences, it may be appropriate to distribute various regulations, such as a security guide, or extracts from the command's security SOP.

c. Refresher Conference. The third phase is the refresher conference or conferences. These should last at least 30 minutes and should occur every 6 months or, as a minimum, yearly. The refresher conference should be designed to satisfy three requirements:

(1) Remind the individuals of their continuing security responsibilities.
(2) Answer the questions which individuals may have about security practices or procedures.
(3) Serve as a vehicle for explaining new changes or requirements in the field of security.

d. Security Reminders. The fourth phase is the use of security reminders. As an indirect approach to indoctrination, security reminders bring to the attention of individuals their security responsibilities during the normal course of their duties.

e. Security Promotion. The fifth phase is security promotion. An active security promotion program vigorously supported by the command is an effective method of maintaining security awareness. Security promotion fulfills two requirements:

(1) Provides the command with a method for recognition of individual achievement in promoting security.
(2) Increases the security consciousness of the command through group participation.

f. Special Interviews. The sixth phase is the special interview. Supervisory personnel should be given a special interview. This special interview should be accomplished in order to obtain the following objectives:

(1) A supervisor should recognize and make on-the-spot corrections of faulty or careless practices.
(2) The supervisor should set the example in sound security practices and procedures.
(3) The supervisor should demonstrate a healthy attitude toward security.

g. Debriefing. The last phase of a security education program is debriefing. Security debriefing is required whenever a person who has had access to classified information leaves the command. Consideration should also be given to conducting a debriefing upon the completion of specific classified projects. The security debriefing serves two purposes:

(1) Special notice to the individual of his continuing responsibility to protect classified information of which he has knowledge.
(2) Command assurance that all classified documents and other classified material with which the individual was charged have been properly accounted for.

10-22. Sources of Material

In order for any security lecture or security conference to be effective, appropriate and pertinent material must be presented to the participants of the conference or lecture. There are many sources of material available to the average counterintelligence unit. A wealth of information can be extracted from the files of the unit itself. In the selection of this material, it is necessary that only facts of educational value and motives of interest to the audience be selected. If actual cases are used as examples, they must be condensed, sanitized, and approved for release. Newspaper articles as well as the dead files of local newspapers provide a wealth of information that can be used in security lectures or conferences. A large number of books and articles concerning intelligence, espionage, and security have been published. Carefully selected extracts from these books make the security lecture interesting as well as pertinent. Security skits are particularly effective because they can be tailored individually to fit any given situation.
CHAPTER 11
COUNTERINTELLIGENCE TECHNICAL SURVEYS AND INSPECTIONS

Section I. GENERAL

11-1. Definition and Purpose

a. A counterintelligence technical survey is a service provided by counterintelligence units to assist commanders in determining the physical and electronic security measures necessary to detect or neutralize attempts at clandestine surveillance through audio and visual means in locations where classified defense information and official information of a nondefense nature is present.

b. A CI technical inspection is a service performed by counterintelligence units to assist commanders in determining the effectiveness of established technical security policies and procedures. The CI technical inspection verifies compliance with recommendations of previous technical surveys and inspections to insure the elimination of technical security hazards and provide technical support of limited scope or duration.

c. Locations where technical surveys and inspections may be desired include, but are not limited to, offices, war rooms, and conference rooms. Information which may be of value to an intelligence service or foreign government includes not only classified defense information, but also information concerning personality traits, habits, interests, and family relationships of military and civilian personnel assigned to sensitive positions.

d. Technical surveys and inspections are conducted when requested by a commander or directed by higher authority. Sensitive areas in relatively constant daily use should be surveyed or inspected at irregular intervals of sufficient frequency to afford maximum security from clandestine audio and visual surveillance. A technical survey or inspection should not be included as an integral part of a CI survey or inspection.

11-2. Scope

a. Technical surveys and inspections will deal with items of technical security only as they are related to counterintelligence. Since there could be a degree of overlap with the programs under the monitorship of the Provost Marshal General and the Chief, United States Army Security Agency, there should be coordination with those agencies.

b. A technical survey or inspection is a complete and detailed examination of all factors, positive and negative, which affect the audio and visual security of the location or equipment being serviced.

c. Technical surveys will include the following:

(1) A complete physical, visual, and electronic search for unauthorized modification of equipment normally found in the area.

(2) A complete physical, visual, and electronic search for clandestine technical penetration equipment.

(3) All procedures necessary to detect the presence of conditions which may allow an unauthorized transmission of any conversation out of the area or surveillance of any activity occurring within the area under search.

d. Technical inspections are more limited in scope than technical surveys, and are designed to include those actions and procedures necessary to provide the requested service. Examples of activities which may constitute a technical inspection are:

(1) Physical and electronic examinations of critical equipment such as telephone wires and instruments, intercommunications systems, and furniture and hardware prior to placement in the area. This is done to prevent an unauthorized modification and possible use for clandestine surveillance.

(2) Electronic examinations and tests scheduled at irregular intervals as a followup inspection of an area previously cleared.

(3) Electronic security monitoring activities in the vicinity of sensitive areas during conferences wherein classified material is presented.
Section II. CONDUCT OF COUNTERINTELLIGENCE 
TECHNICAL SURVEYS AND INSPECTIONS

11—3. Technical Survey

a. Prior to the actual commencement of the technical survey, liaison will be established with the installation to be surveyed to determine pertinent factors which will assist in the conduct of the survey. This will be accomplished by a conference among the survey team Special Agent-in-Charge, the commander of the installation to be surveyed or his designated representatives, and the installation's communication officer. This conference will acquaint the commander with the proposed scope of the survey and will establish the requirements for cooperation by members of the installation. It will include a guided tour of the area to be surveyed and will, in addition, include arrangements for acquiring access to desks, containers, secured areas, and outside perimeter areas in which related communication, electrical, heating, and plumbing junction facilities are located. It should be emphasized by the Special Agent-in-Charge that upon completion of the survey the area must be afforded physical security commensurate with the highest classification for which the area is to be used. At this time, any limitations placed on the conduct of the survey by the local command should be clarified. One limitation that should always be considered is the actual dates and time of the survey which should be classified as CONFIDENTIAL, and annotated FOR EYES ONLY for the key personnel, e.g., commander, G2/S2, and perhaps the G3/S3.

b. Technical survey team members will familiarize themselves with the entire installation to be surveyed in order to obtain an overall estimate of existing factors which will provide a guide for the detailed conduct of the survey. The files of the counterintelligence unit are often valuable sources of information relative to the installation. Reports of previous CI surveys will contain detailed information concerning the security measures of the installation and a description of the surrounding area, including natural and structural elements, which may tend to enhance either audio or visual access to the area, or point out any limitations imposed on the previous survey team. Detailed construction blueprints, as well as heating, electrical, and communications details, should be obtained if possible. In addition, ground maps indicating overhead and underground utility networks should be available to the survey team as required.

11—4. Preparation of Checklist

A technical survey consists of a thorough physical search and full utilization of available electronic and specialized detection equipment and devices. The sensitivity of the area, the availability of qualified personnel and technical equipment, and consideration of the time factor will of necessity affect the thoroughness and efficiency of the technical survey. Continuing developments in the electronic surveillance field make it impractical to set forth a definite step-by-step survey procedure which may soon be outmoded. Personnel who are specially trained in audio surveillance countermeasures should be utilized to the fullest extent possible in planning and conducting a technical survey. Each counterintelligence unit should prepare a general checklist to be utilized in conducting a technical survey. The checklist will insure that all aspects of the survey are thoroughly and systematically accomplished; however, the checklist should not restrict the initiative of the technician. A sample general checklist, which may be used as a basis for preparation of a checklist, is contained in FM 30–17A, the classified supplement to this manual.

11—5. Detection Equipment

Various types of specialized electronic equipment are available to counterintelligence technical personnel to assist in locating concealed clandestine surveillance and listening devices. The Intelligence Materiel Support Office, under the control of the US Army Intelligence Command, Department of the Army, provides funds for certain special items. Sufficient reference material, periodical literature, and technical information bulletins should be procured by units in the field in order to keep abreast of the latest developments in electronic equipment. Requests for information on, or development of, specific items of electronic equipment should be forwarded through channels to the Intelligence Materiel Development Office, Fort Holabird, Maryland 21219.

11—6. Technical Inspection

The general provisions concerning responsibilities and planning for the conduct of technical surveys (para 11—3—11—5) apply equally to the conduct of CI technical inspections.
11-7. Discovery of Clandestine Surveillance and Listening Devices

When discovery of a clandestine surveillance and listening device is made, a report should be submitted immediately as outlined in AR 381-14. Counterintelligence units should have a SOP which will delineate the action to be taken by counterintelligence personnel upon discovery of a clandestine surveillance device. It is essential that all audio surveillance countermeasures technicians be thoroughly familiar with the instructions contained in AR 381-14. The discovery of a clandestine surveillance or listening device may have an impact extending to the highest national levels.

11-8. Reports

Counterintelligence technical survey and inspection reports are prepared in accordance with reporting procedures discussed in chapter 10. These reports will include technical data which contributed to the conclusions reached in the technical survey or inspection. An additional section, "Limitations," is normally added to the five sections discussed in chapter 10. A sample report of a CI technical survey is contained in appendix C.
CHAPTER 12
CONVENTIONAL COMBAT OPERATIONS

Section I. INTRODUCTION

12-1. General
The field army is provided counterintelligence support by a counterintelligence company at field army level in the MI Battalion and by counterintelligence elements which are organic to military intelligence units attached to corps, divisions, and separate brigade-sized organizations. These counterintelligence elements and units contribute to the mission of the commander at each echelon by assisting him in carrying out his counterintelligence responsibilities.

12-2. The Counterintelligence Mission in Tactical Operations
The counterintelligence mission stated in chapter 1 of this manual is valid for all operations. Emphasis on certain aspects of the mission will change with the tactical situation and will vary with the echelon of command. Denial of information to the enemy is one of the most important aspects of the counterintelligence mission at the tactical level and receives greater emphasis during actual operations.

Section II. FUNCTIONS

12-3. Introduction

a. Counterintelligence operations are aimed at defeating the collection capability of the enemy. In rear areas, overall security is indispensable to effective support and control of combat forces. The enemy can be expected to exploit the loose demarcations of the battlefield by the deep penetration of espionage-sabotage elements, the subverting of selected elements of the indigenous population, and employing guerrilla forces to the maximum extent. To counter these threats, counterintelligence elements must work aggressively in close coordination with such related activities as psychological warfare, military police, civil affairs, and air defense units.

b. Counterintelligence operations within the field army under tactical conditions will consist generally of the following:

(1) Personnel security. Background investigations will continue. Close coordination between military and civilian agencies which control pertinent files must be developed to maximize the effectiveness of these investigations.

(2) Physical security. Counterintelligence personnel must provide installation and unit commanders with survey and inspection services to insure protection against physical penetration and compromise of classified information and material. The mobility and frequent displacement of installations, their proximity to the indigenous population, and the complications presented by combined operations with diverse allied forces will compound the security problem. Any recommendation on the use of unattended ground sensors by a unit for physical security should be coordinated with the unit sensor officer to determine his capabilities in this area.

(3) Special weapons security. Special weapons and associated systems within the field army will require increased security efforts on the part of both counterintelligence and other agencies during use, storage, and transport of system components.

(4) Civil security. Local civilian elements as well as refugees, displaced persons, and indigenous employees of US Forces, will be lucrative targets for recruitment by enemy forces for espionage, sabotage, and subversion.

(5) Counterespionage, countersabotage, and countersubversion. Individuals and groups with espionage, sabotage, and subversion missions must be identified, located, penetrated, and/or neutralized (FM 30-17A).
12-4. Operations in Forward Areas

a. Offensive Operations.

(1) In the attack, emphasis must be placed on the neutralization and/or exploitation of CI targets which are known to exist in enemy-held areas as reflected in target lists (see FM 30-17A). To accomplish this task effectively, counterintelligence personnel supporting combat units may be deployed to forward elements as required by the mission. Initial advance by combat troops through the objective area may be desired prior to the commitment of counterintelligence personnel in forward areas. Flexibility must be maintained in order to obtain maximum use and effectiveness. Counterintelligence needs and requirements vary constantly and personnel may be deployed from one unit to another and from forward to rear areas as these conditions change.

(2) Counterintelligence personnel operating with forward combat units perform their mission within the existing boundaries of the supported unit. When rear boundaries are advanced, control of the relinquished area will be assumed by the counterintelligence elements gaining responsibility for the area. All documents and files pertinent to the area will be physically transferred, as will any personnel held in custody. The gaining element must be thoroughly briefed on affairs of CI interest in the relinquished area.

b. Defensive Operations. In the defense, counterintelligence elements in forward tactical areas will be most active in combating enemy intelligence efforts to obtain information and intelligence concerning US Forces. Enemy intelligence activities may take many forms during this phase of operations.

(1) Deployment of counterintelligence personnel normally will differ from that undertaken in the attack. In most cases, deployment will be in rear areas rather than forward with the combat units; however, counterintelligence personnel will be prepared to operate whenever and wherever indications of enemy activities require a counterintelligence effort. In the defense, emphasis will be placed on such functions as:

(a) Civilian and prisoner of war screening and interrogation.

(b) Development of effective human source programs (FM 30-17A).

(c) Security of critical installations and activities.

(d) Continued briefings of military police, civil affairs personnel, and G2/S2 staffs on hostile intelligence activity and modus operandi.

(2) Enemy guerrilla forces activities and operations against installations, supply points, lines of communications, and other critical areas will increase during defensive operations.

(3) In the defense, forward area counterintelligence elements may initiate certain special operations designed to collect intelligence information or assist the commander in a specific operation directed against enemy forces. These operations require careful and detailed planning (FM 30-17A) and will be controlled and monitored by higher commands. Examples are as follows:

(a) Recruitment of confidential sources and their injection into refugee groups and prisoner of war channels.

(b) Exploitation of known enemy intelligence agents.

(c) Use of deceptive information as directed by higher commands.

c. Retrograde Operations.

(1) Counterintelligence operations must be compatible with the courses of action taken by the supported combat unit. In a retrograde movement, the security of troop movements and lines of communication is a paramount consideration. Other considerations include:

(a) Evaluation of white and black list (see para 12-9) personnel.

(b) Evaluation of prisoners of war of CI interest.

(c) Evaluation of confidential sources who cannot remain behind for either operational or security reasons.

(2) In conjunction with military police, rigid controls over civilians and refugees must be applied to detect persons posing a threat to the security of friendly operations. Command post areas which have been evacuated will be inspected by counterintelligence personnel to insure that no information or material has been left behind which might benefit hostile forces.

(3) During retrograde operations, the transfer of areas of responsibility occurs in reverse of that for offensive operations. The forward element will establish contact with that element responsible for the CI coverage of the rear area which it will occupy; receive a briefing concerning operations in that area; and receive applicable files, documents, and personality information on sources and other persons of potential CI value within the area.
12-5. Rear Area Operations

a. Counterintelligence Area Coverage.

(1) Counterintelligence area coverage refers to counterintelligence responsibility applied throughout a geographic area for which a specific commander may be responsible. In a theater of operations, with an army commander as the unified commander, US Army counterintelligence has the responsibility of conducting all operations within the CI mission necessary to the security of the command. A unified commander from another service may assign US Army counterintelligence units an area coverage mission. Counterintelligence units may have investigative jurisdiction over the activities of indigenous civilians and US civilians employed by, or accompanying, the Armed Forces, in addition to the normal jurisdiction of Armed Forces personnel.

(2) Counterintelligence area coverage throughout a divisional area is provided by the counterintelligence personnel of the division military intelligence company. This same coverage is provided in the area extending from the division rear boundary to the field army rear boundary by the MI Company (CI) assigned to the MI Battalion (Field Army). Counterintelligence area coverage from the field army rear area boundary throughout the communications zone is provided by the MI Group (CI) of the Area Support Command (ASCOM).

(3) Unless the commands to which they are assigned or attached are employed separately, CI elements of the MI unit supporting corps, army groups, and separate support commands normally will not be assigned a CI area coverage mission. Their efforts will be directed toward contributing to the internal security of the respective supported command and participating in counterintelligence planning.

b. Rear Area Security. Rear areas may be defined broadly as those areas in which combat service support activity is accomplished. Enemy attacks against administrative support units and installations, lines of communications, and vital communications centers in rear areas, may jeopardize the primary mission of combat forces. The objective of rear area security is to prevent serious enemy interference with all operations in rear areas. By the very nature of their mission, CI elements provide area coverage and are in a position to provide valuable assistance to supported commands in countering enemy activities in these areas. Specific CI activities in support of rear area security may include:

(1) Collection and collation of information concerning key personalities among hostile elements operating in rear areas.

(2) Conduct of operations designed to effect penetration of hostile intelligence services at all echelons.

(3) Development of civilian human source networks dispersed throughout rear areas, which will provide timely and pertinent information.

(4) Application of surveillance techniques to known, suspected, or potential hostile bases of operations.

(5) Search and seizure operations against hostile personalities, installations, organizations, or those sympathetic to the hostile cause.

(6) Conduct of CI security and technical surveys and inspections of US and, if directed, allied installations in US rear areas.

(7) Assistance to rear area security elements in the denial of known, suspected, or potential sources of food, supply, or other support to hostile groups.

(8) Assistance to and support of the continuing program of security orientation and indoctrination of all command personnel, with emphasis on the provisions of AR 381-12.

(9) Contribution to, or, if directed, preparation of, recurring memoranda to all command echelons concerning current trends or modus operandi of hostile intelligence.

(10) Contribution to, or, if desired, preparation of, portions of command policy documents concerning countersubversion and countersabotage.

(11) Preparation or recommendation of specific CI measures to unit and installation commanders for the enhancement of security practices to include such items as the detection of behavioral patterns detrimental to the security of the command.

c. Special Situations. Assignments demanding a high degree of alertness, flexibility, and resourcefulness on the part of counterintelligence personnel may include—

(1) Areas where the populace is basically hostile to US interest.

(2) Areas especially vulnerable to insurgency activities.
(3) Areas in which targets of known enemy high-priority collection tasks (or interest) are located.

12—6. Other Tactical Operations  

a. Counterintelligence personnel may be required to provide CI support for other tactical operations. Normally, CI elements will be attached to the supported unit for the duration of the operation and tailored to meet the demands of the specific operation. Airborne, amphibious, separate task force, and internal defense/development operations (chap 13) will require varying degrees of CI support and participation. In addition, CI support and assistance may contribute materially to the success of unconventional warfare operations by furnishing timely and accurate information related to enemy-occupied territory into which operations are planned.  
b. In most special tactical operations, the security of the operation itself, from the time of inception to the time of initiation, is of utmost importance. Counterintelligence efforts, in conjunction with G3 personnel will be directed toward denying the enemy access to information concerning the time, destination, and objectives of the mission during the planning and preparation phase. Measures to be considered include:
   (1) Increased emphasis on counterespionage activities (FM 30–17A).  
   (2) Increased security indoctrination and training to include CI security and technical inspections.  
   (3) Rigidly controlled security measures to include restriction of personnel, if necessary.  
   (4) Security of training, logistical and reconnaissance activities as well as other preparations or activities which could indicate pending operations.  
   (5) Security of assembly and departure areas to preclude infiltration of unauthorized personnel, and provide for maximum reduction of casual observation opportunities.  
c. During the operation itself, the amount and type of CI support required will be influenced by the size and scope of the operation, the objective area and the location and availability of CI targets. The deployment of counterintelligence personnel will be dependent upon the targets to be neutralized or exploited in the objective area.

Section III. PLANNING AND CONDUCT OF OPERATIONS

12—7. Introduction  

Counterintelligence planning is accomplished concurrently with the planning and conduct of theater army operations plans and policies. Within that broad framework, CI plans at lower echelons will be increasingly detailed but flexible. All aspects of CI activities required to insure adequate direct support for all phases of operations of the supported units will be considered. The effectiveness of counterintelligence operations in tactical areas depends largely upon the planning preceding the operation. FM 30–5 contains examples of the plans utilized by counterintelligence personnel.

12—8. Target Selection and Priorities  

a. The selection and assignment of CI targets should be based on an assessment of the overall hostile threat. This assessment is the responsibility of the G2, Theater Army, and should take into consideration both the immediate and obvious threats to security as well as future threats which can be anticipated. A thorough CI target analysis should encompass the relatively permanent features and fundamental characteristics of a country, area, or broad special subject to include the political, economic, military, and sociological aspects.

b. Numerical priority designations which emphasize the relative importance or value of CI targets and which designate to the responsible unit(s) the degree of interest expressed by the requester will be influenced by:
   (1) Security threat posed by the target.  
   (2) Relative urgency of need for the neutralization or exploitation of the target.  
   (3) Capabilities of the units responsible for accomplishing the tasks.  

Priority designations which have been established at theater level and forwarded to lower echelons will not be altered. Local CI elements may assign priorities to targets locally developed. Counterintelligence personnel must adjust their daily operations to conform with the established priorities.
Counterintelligence targets include personalities, installations, organizations, groups, documents and materiel. Information on these targets can often be obtained through civil affairs units or Civil-Military Operations Staffs, G5/S5. Civil affairs units are also principal users of this type of intelligence.

a. Personalities.

(1) Black list. Black lists are developed or compiled at all echelons of command and contain the identities and locations of individuals whose capture and detention are of prime importance to the US Army. Black lists include—

(a) Known or suspected enemy or hostile espionage, sabotage, political, and subversive individuals.

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

(c) Political leaders known or suspected to be hostile to the military and political objectives of the United States and/or an allied nation.

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

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

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

(g) 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/or national departments or agencies.

(2) Gray list. Gray lists, which are compiled or developed at all echelons of command, contain the identities and locations of those personalities whose inclinations and attitudes toward the political and military objectives of the United States 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. They may be individuals whose political motivations require further exploration before they can be utilized effectively by US Forces. Examples of individuals who may be included in this category are:

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

(b) 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.

(c) Nuclear scientists, physicists, and technicians suspected of having been engaged in enemy nuclear research projects or nuclear missile programs against their will.

(3) White lists. White lists are compiled or developed at all echelons of command and contain the identities and locations of individuals in enemy-controlled areas who have been identified as being of intelligence or CI interest and are expected to be able to provide information or assistance in the accumulation of intelligence data or in the exploitation of existing or new intelligence areas-of-interest. They are usually in accord 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:

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

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

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

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

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

b. Installations. The installation target is any installation which is of interest or poses a threat to the security of US Forces in the area. These installations provide information of significant value if exploited; they can also pose a definite threat to our security if improperly treated. Continued operation of these installations during combat operations may jeopardize the com-
mander's successful accomplishment of his mission. Installation type targets of interest to the military commander, and of immediate concern to counterintelligence, can be found in any average town or city regardless of its location. Examples of installation type targets are as follows:

1. Civilian communications media.
2. Enemy signal communications centers.
3. Nuclear research centers and chemical laboratories.
4. Installations formerly or currently occupied by enemy espionage, sabotage, and subversive agencies, or enemy police organizations, to include prisons.
5. Installations occupied by enemy intelligence or security organizations.
6. Ordnance repositories.
7. Embassies and consulates of hostile governments.
8. Military installations.

c. Organizations and Groups. Any organization or group which is an actual or potential threat to the security of US or allied forces must be neutralized. The threat which an organization or group presents may not be immediately apparent to the military commander, the G2, or the counterintelligence unit. The enemy will frequently camouflage his espionage or subversive activities with the establishment of front organizations or groups which, if permitted to remain in being, could impede the success of the military operations. Examples of hostile organizations and groups which are of major concern to the counterintelligence unit during tactical operations are as follows:

1. National and local political groups and parties known to have or suspected of having aims, beliefs, or ideologies contrary or in opposition to the United States.
2. Paramilitary organizations to include student, police, militia/veterans, and excombatant groups known to be hostile to the United States.
3. Hostile sponsored groups and organizations whose objectives are to create dissension and spread unrest among the civilian population in the theater of operations.
4. Headquarters, provincial, and municipal offices of those hostile organizations indicated by the theater commander as subject to immediate neutralization. Personalities related to those offices should be arrested and detained.

12–10. Neutralization and Exploitation

a. Operational Support.

1. Tactical troop augmentation. Counterintelligence elements involved in tactical operations do not have the capability to provide guards or take under physical control those CI targets from which hostile resistance continues. The MI unit commander must, in his planning, estimate his needs far enough in advance so that requests for additional personnel or assistance in the objective areas are made known to the G2 of the major command prior to an offensive operation. The G2 will arrange to obtain those personnel necessary for the accomplishment of the mission. Once entry has been made into the target area by counterintelligence personnel, a preliminary search has been completed for information of intelligence or CI value, and the employees or occupants
have been located or detained, the physical guarding or control of the target is turned over to guard personnel or the service or agency with primary interest in the target. How and when troops are assigned specific guard functions around these CI targets will be influenced by local requirements. In some instances, guard personnel may accompany Special Agent teams to the target area; in other cases, they may rendezvous with the teams in the target area. It must be understood, however, that the tactical effort, except in unusual cases, takes precedence over CI target neutralization and exploitation. If tactical troop augmentation is not possible, the CI element may have to rely on its own limited capabilities to neutralize or exploit the targets.

(2) Civil police support. Counterintelligence elements involved in tactical operations may request and receive support from civil police agencies in friendly controlled territories. Normally, this support is arranged through the G2 in coordination with the G3 or G5. Civil police may be utilized to accompany Special Agent teams on target neutralization missions, assist in apprehensions of target personalities, and provide guards for installations which have been neutralized. Considerable time and effort may be saved in the performance of the counterintelligence mission if good liaison and working relationships can be established with the local civil police forces.

b. Target Personalities. The processing of target personalities apprehended by CI elements operating in tactical areas will generally be accomplished according to procedures established by field army. In most cases prisoners of continuing CI interest apprehended in forward combat areas will be evacuated as soon as possible to higher echelons. It is essential that such prisoners not be lost in the stream of other prisoners captured by the tactical units. The tactical situation may not permit the immediate routing or "evacuation of target personalities, but it may be possible to temporarily secure the prisoner in a local jail or prison. Counterintelligence prisoners should not be permitted to come into contact or associate with the other prisoners. A record of prisoners incarcerated temporarily must be forwarded to field army so that action may be taken, when the tactical situation permits, to interrogate and make disposition of the prisoners. Target personalities often prove to be valuable sources of combat and strategic intelligence information. Action should be taken to promptly elicit all information of immediate tactical interest to friendly forces, and to make these persons available for interrogation by other agencies. Black and gray list personalities are not expected to be cooperative under interrogation; however, counterintelligence personnel should be alert to indications that these individuals may cooperate in return for preferential treatment.

c. Target Installations. The exploitations of installation targets may be accomplished immediately following the neutralization of the installation by counterintelligence personnel, or at a later date if exploitation is not immediately possible due to the tactical situation or for other reasons. During the exploitation phase, the installation will be searched thoroughly for documents, equipment, and materiel of intelligence or CI interest. Disposition instructions concerning documents and materiel captured by counterintelligence personnel while involved in tactical operations will be found in command SOP or in FM 30–16. Documents, to include files and records, should be evacuated only through intelligence channels. In some instances, it may be advisable or desirable for the documents or materiel to remain within the installation, building, office, or billet where found until such time as they can be thoroughly examined or analyzed by other counterintelligence or technical intelligence personnel.

12–11. Tactical Counterintelligence Interrogations

a. General. The circumstances of combat and the counterintelligence operations in tactical areas complicate the task of the Special Agent interrogator. There may be overwhelming numbers of people who are looked upon as threats to security, perhaps solely due to their presence in the combat zone. The number of suspect personnel will vary, but it frequently will be large enough to preclude detailed interrogation of all but a selected few. Counterintelligence personnel will be partly dependent on such agencies as the provost marshal, Civil Affairs (CA) units, and prisoner of war interrogators to identify suspect persons or persons of CI interest. In some situations, the number of persons volunteering information to counterintelligence personnel will be large enough to necessitate a preliminary screening operation to permit concentration on those of the greatest potential interest or value. Most suspects are apprehended as they try to enter or leave a zone of operations. If they are in fact enemy agents, they will have cover stories closely paralleling their true environments and identities. The
Special Agent's success in such interrogations will be dependent primarily on his questioning skill, linguistic ability, knowledge of the area of operations and adjacent areas, and familiarity with the intellectual, cultural, and psychological peculiarities of the persons encountered.

b. Types of Subjects. 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 categories of persons are of CI interest:

1. Refugees and displaced persons.
2. Line crossers.
3. Deserters from enemy units.
4. Civil prisoners and enemy prisoners of war.
5. Inmates of concentration camps.
6. Repatriated prisoners of war and escapees.
7. Members of underground resistance organizations seeking to join friendly forces.
8. Collaborators with the enemy.
9. Target personalities, such as black, gray, or white list personalities.
10. Volunteer informants.
11. Persons who must be questioned because they are under consideration for employment with US Forces or for appointment as civil officials by CA units.

c. Other Interrogations. If the security of US personnel, units, installations, and military operations is to be maintained, the threat posed by the civil population must be ascertained. Relatively large scale interrogations of civilians may be necessary to ferret out concealed enemy agents. Civilians are also a source of tactical and strategic intelligence as well as counterintelligence information. In a combat area persons are often eager to denounce neighbors or acquaintances for personal reasons or gain; much of this information may be of little value.

d. Objectives of Counterintelligence Interrogations. The counterintelligence interrogation in combat areas assists in the accomplishment of three major objectives.

1. In the screening process, the Special Agent helps remove from the battlefield the refugees whose very presence threatens overall security.
2. In detailed interrogations, the Special Agent detects enemy agents with espionage or sabotage missions.
3. The wide range of his activities permits the Special Agent to collect information of value to other intelligence and security agencies and the planners of military operations. He must be especially alert to obtain and report information of immediate tactical value which was not gleaned from the refugee by prisoner of war interrogators.

e. Indicators Warranting Suspicion. Because the Special Agent usually lacks positive evidence and obtaining confirmation of a suspect's story is an improbability, he must be alert during interrogations for indications of espionage or agent activity. Indications which separately or collectively may give rise to the suspicion that a subject is in the employ of, or acting in sympathy with, enemy forces are as follows:

1. Access to information or targets. A prospective espionage or sabotage agent must have access to the information desired by the enemy or the target installation to be destroyed in order to carry out his mission. Hence, the interrogation should establish a subject's accessibility to potential targets, including his location at the time he was apprehended.
2. Technical skills. Proficiency in certain technical skills is frequently an attribute of an espionage or sabotage agent. The subject who has a mastery of one or several foreign languages, a knowledge of radio operation or of cryptography should be questioned carefully on the nature and purpose of his training in those fields. His practical experience and his work in those fields during or shortly prior to the war should give the Special Agent cause for strong suspicion, and the individual's story must be closely examined. Technical advice for the interrogation of such individuals should be obtained from USASA elements.
3. Documents and funds. An overabundance of documents and “new” documents of questionable authenticity give reason for doubt and should be the basis for detailed questioning. Discrepancies in document's contents or conflicts between data and the subject's story have frequently led to detection of hostile agents. Unexplainable possession of large amounts of money, valuable jewelry, or other items of great value should be questioned carefully.
4. Pro-enemy background. Residence or travel in enemy territory, membership in a hos-
tile party, or known former collaboration with the enemy are facts of obvious importance. The Special Agent must determine whether the subject is actually in sympathy with the enemy or has acted merely to serve his own best interests with regard to his life, the welfare of his family, or his property.

(5) Family in enemy-held areas. Enemy pressure is often applied to individuals whose families reside under enemy control; particularly, if the family had no past connection with the enemy-held area.

(6) Inconsistent story. Small discrepancies in the subject's story may be important. Distance compared to travel time, accent peculiar to an area the subject refuses to acknowledge as his own, unreasonable explanation of deferment, exemption, or discharge from military service, exemption from labor conscription, or implausible reasons for risking the crossing of battle lines may be warning signals to the counterintelligence interrogator. Contradictions in a subject's story do not warrant jumping to conclusions; however, the Special Agent must remain alert to all possibilities. Allowances must be made for defective memory or lack of logic due to the emotional stress of a subject.

(7) Suspicious actions or activities. Unusual interest displayed by indigenous persons in troop units or equipment, or persistent loitering in the vicinity of troop units and installations without reasonable explanation should be sufficient to warrant interrogation for the purpose of clarifying the status of a person so involved.

(8) Violations of civil or military regulations. Mere violation of military regulations in an area controlled by the military, such as mandatory registration, curfews, travel restrictions, or declaration of weapons, may be relatively unimportant to CI elements. However, the motives which such violations despite severe penalties must be compelling, and may possibly be of great interest to counterintelligence personnel.

(9) Modus operandi. The frequent similarity of tactics of hostile agents working for the same enemy agency or force, means of contact with their agent handlers, type of cover story, and manner of collecting and reporting their information may lead to identification of suspects with a known enemy agency or group. Established patterns of activity or behavior of enemy agents should be disseminated to all intelligence and security agencies to assist in the identification of agents still operating.

f. Screening or Preliminary Interrogation. Preliminary interrogation and screening are generally synonymous, except that the former indicates that there will be a followup detailed interrogation, while screening involves the selection by brief questioning of a relatively small number from a large group for detailed interrogation (para 12-16). In both cases the technique, purpose, and scope of the questioning are generally the same. The object is to select for detailed interrogation a reasonable number of persons who appear to be suspect or knowledgeable on matters of CI interest. Preliminary interrogation or screening is generally concerned with identity, background, recent activities, and travel or escape routes. Arrested civilians who are to undergo preliminary interrogation or screening must first be searched for weapons and evidence; the life of the Special Agent and the success of the preliminary interrogation may depend on it. Documents and personal belongings of a subject must be examined; the circumstances of apprehension, if by personnel of another unit, must be studied. Available files should be checked. Counterintelligence units normally prepare a standard screening report form to serve as a guide and convenience for the Special Agent. Circumstances at the time, number of persons to be screened, and number of Special Agent interrogators available will dictate the length or detail of the screening. Generally, the following items will be the basic data to be developed during screening or preliminary interrogation:

  (1) Subject's name and aliases.
  (2) Date and place of birth.
  (3) Nationality, past and present.
  (4) Family, complete with addresses.
  (5) Education.
  (6) Technical skills.
  (7) Occupation.
  (8) Places of residence with dates.
  (9) Religion.
  (10) Political affiliations.
  (11) Military history.
  (12) Wartime activities.
  (13) Circumstances preceding apprehension.
  (14) Reason for presence in the area.
  (15) Information of counterintelligence or intelligence interest.
In large scale screening operations, shortage of time may be a critical factor. It may be advantageous to have the subjects fill out forms if they are able to do so. A study of the form with questions on any suspicious entries must follow; however, well trained professional agents will rarely be exposed by use of this technique. If detailed interrogation appears to be warranted, the subject is isolated for evacuation or transportation to the appropriate interrogation site. This rule applies not only to suspects but to persons with an abundance of information of counterintelligence or intelligence interest. A copy of the screening report should accompany the subject to the next interrogation site.

9. Detailed Interrogation. Detailed CI interrogations may be conducted in joint interrogation centers (FM 30-15) or at interrogation sites established by intelligence units (usually at field army or higher level). Detailed interrogation does not differ radically from the preliminary interrogation except that attention is now focused on individuals who are suspect or who are known to have extensive information of interest. A study of the preliminary interrogation or screening report, examination of the subject’s documents and belongings, and checks of available files and information must be conducted and analyzed in preparation for the interrogation. The Special Agent then proceeds with the interrogation using techniques discussed in FM 30-15.

(1) Details of the subject’s personal history must be reviewed. Should the subject confess that he is an enemy agent, he becomes an important source of information on hostile intelligence methods of operation and, perhaps, on identities of other hostile agents, unless, of course, he is a confusion agent. This will lead to exhaustive interrogations on such issues as hostile intelligence, operations, identities of agents, the manner of his recruitment, training he received, missions he was assigned, and those he accomplished.

(2) The suspect or any person being interrogated may also be an important source of information of intelligence value, strategic or tactical.

(3) The questioning usually should follow a logical sequence to avoid confusing the subject and to facilitate reporting. An illogical sequence may be used as a technique to purposely confuse the subject so that he will inadvertently contradict himself. The Special Agent must be alert for discrepancies. He must retain his psychological advantage.

12-12. Investigations and Internal Security Functions

There are certain unique additional problems that may confront counterintelligence personnel while conducting investigations and services in a tactical environment.


(1) Counterintelligence elements are responsible for conducting security investigations of indigenous personnel retained in their official civilian positions and of other civilian personnel to be employed by the US Army in a theater of operations. The scope of investigation normally will depend on the position or job for which the person is applying and the degree of sensitivity and access to classified defense information. AR 604-5 discusses details concerning the conditions under which indigenous employees may be granted access to classified defense information. The final decision on employment clearance remains a command responsibility. Difficulty may be often encountered by the Special Agent because of lack of files, records, and other repositories of civilian police and other investigative agencies which have been destroyed or displaced as a result of tactical operations. Every attempt must be made to check all files and records which may be available. Utilization of indigenous personnel by US Forces presents a definite security threat because of enemy penetration efforts utilizing indigenous civilian employees who are sympathetic with, or may be coerced into serving, the enemy cause. Caution must be exercised by all using units to preclude compromise of classified information. A threat just as serious is posed by the capability of employees to collect volumes of unclassified information on planned movements or tactical operations of US units. Any indication of disloyalty or other suspicious conduct on the part of the indigenous employee will be reported immediately to the intelligence officer of the command through appropriate channels. Once a labor pool of cleared indigenous personnel has been established in the command, units normally will hire only from this pool. The command should publish an SOP concerning hiring, utilization, and control of indigenous personnel. Civil affairs under the staff supervision of the Assistant Chief of Staff for Civil-Military Operations (G5) has the responsibility for providing labor for military forces and coordinating with CI elements concerning measures to provide necessary security screening of indigenous personnel considered for employment. Counterintelligence elements
will maintain a close working relationship with CA elements and Civil-Military Operations staffs at all echelons within the theater. The security problem does not end with clearances. A close continuing watch or check on employees must be maintained.

(2) Counterintelligence personnel frequently must rely on qualified indigenous civilians or members of allied forces to serve as interpreters and translators. Properly utilized and controlled, indigenous interpreters have proved to be of great value to CI operations. They are capable of detecting dialect differences and discrepancies in civilian accounts of incidents or circumstances and are frequently more discerning in interrogations dealing with local civilians and hostile intelligence agents. They familiarity with the country in terms of regional, religious, social and political schisms, attitudes, and prejudices represents skills not easily developed by counterintelligence personnel from a different environment. On the other hand, these same advantages may influence interpreters’ work and color their reports. Indigenous employees of CI elements must be strictly controlled by Special Agents. Overfamiliarity, lack of restraint, freedom of movement, and independent actions on the part of the indigenous employees are unacceptable. FM 30-15 discusses the use of interpreters and the necessity for security clearances.

b. Riots and Civil Disturbances. FM 19-15 outlines the responsibilities of the major commander and the utilization of troops when riots and civil disturbances occur in territories where US troops are stationed by agreement or consent, or in areas occupied as a consequence of belligerent actions. Effective counterintelligence, however, may preclude riots and disturbances. Continuous efforts by counterintelligence with close coordination with the Provost Marshal and the G5 must be made to determine the probable causes of riots and disturbances, locations where they may occur, types, and number of people involved, identities of leaders, and whether the riots or disturbances are enemy sponsored and directed. With this knowledge, the commander can take necessary action to eliminate potential causes of a riot or civil disturbance.


(1) Troop movement security is designed to prevent espionage or sabotage from interfering with the movement of US Forces, insure the element of surprise, and deny information regarding the movement itself, its purpose, implications, and organization. Counterintelligence personnel may be called upon to provide advice and assistance in the planning and conduct of troop movements. Some of the services which may be provided by counterintelligence personnel include—

(a) Acting in an advisory capacity or as assistants to the G2/S2 in the preparation of the CI portion of the movement plan.

(b) Conducting CI surveys and inspections, recommending measures for maximum secrecy, and providing assistance in instructions to unit personnel concerning troop movement security.

(c) Observing the move to report and investigate security violations or other security threats.

(2) Regardless of the type and mode of transportation utilized for the move, the following security measures must be considered:

(a) Mail censorship.

(b) Monitoring or restriction of communication facilities.

(c) Emphasis on security education programs.

(d) Establishment of curfew hours or restrictions.

(e) Conduct of surveillances of areas and facilities which military personnel frequent during off-duty hours and where “loose talk” may be prevalent.

(f) Removal of identifying marks and insignia from clothing, equipment, and vehicles.

(g) Arrangements for storage or destruction of personal diaries, letters, telegrams, and other documents or papers.

(h) Prevention of unauthorized press releases.

(i) Posting of security guards at loading or embarkation areas, critical or congested areas along the route, and off-loading or debarkation sites.

(j) Crating, covering, and guarding material and equipment to conceal its identity and provide protection from unauthorized access during the move.

(k) Examination of departed areas to insure that no information of intelligence value has been left behind which might disclose the destination, identity, and mission of the unit.

(l) Examination of the intended destination for physical security hazards when possible.

(m) Dissemination of false information designed to deceive or mislead the enemy as to
the actual intentions of the move, when approved by the theater commander or higher authority.


(1) Special weapons systems require many sensitive components, as well as ancillary equipment and supporting documents. The security, classification and the sensitivity of these systems, related equipment, and documents dictate the necessity for strict security measures. Counterintelligence personnel assist special weapons unit commanders and others with responsibility for these systems in establishing adequate security measures at special weapons sites for moves of special weapons and munitions, and at storage depots. This assistance is provided in the form of CI surveys and inspections, monitoring of shipments and deliveries to sites or depots, aid in conducting effective security education programs, and coordinating with other units (e.g., military police) responsible for providing security for these systems.

(2) Regulations governing security requirements for special weapons systems provide minimum security standards and criteria for safeguarding the weapons and their components. Counterintelligence personnel involved in special weapons security must be familiar with these regulations, particularly as they pertain to counterintelligence responsibilities (see AR 50–2, AR 50–3, AR 190–60, and AR 611–15).

(3) Special weapons systems are prime targets for sabotage. Counterintelligence personnel conducting investigations of sabotage or suspected sabotage of special weapons systems should request assistance, as required, of technically qualified personnel.

12–13. Files and Reports

Counterintelligence elements engaged in tactical operations are responsible for developing and maintaining their own operational files. These files will be transferred to the CI element gaining area responsibility as tactical elements displace.

a. Operational Files. Information concerning individuals, organizations, and other subjects of CI interest is assembled and maintained by CI elements engaged in tactical operations for the purpose of furthering the investigative and security mission. This information should be kept to a minimum, consistent with operational needs. Operational files maintained may include, but are not limited to—

(1) Personality files on individuals of current or future CI interest.

(2) Impersonal files such as dossiers on organizations and groups of current or future CI interest.

(3) Correspondence and other reports concerning current or pending operations and investigations.

(4) Hold files containing essentially a collection or summary of all CI operational activities and information assembled during the period in which the unit has operated in a particular geographic area.

b. Reports. Counterintelligence units and elements involved in tactical operations will use standard reports and message forms. The basic forms of CI reports are explained in chapter 7 and appendix B.

12–14. Special Operations

The planning and conduct of CI special operations is included in the classified supplement to this manual, FM 30–17A.

Section IV. TACTICAL SUPPORT OPERATIONS

12–15. General

In a combat environment CI elements can support the commander by conducting CI-oriented tactical support operations from the divisional and separate brigade MI units. These missions should not become the bulk of the element's activities for the tactical unit but should be a complement to the other basic CI tasks previously mentioned in this manual. The basic limitations on the use of counterintelligence personnel as outlined in AR 381–150 still apply.

12–16. Counterintelligence Screening Operations

a. General. Counterintelligence screening operations in a conventional combat environment consist of refugee and prisoner of war screening and mobile and static checkpoints which are dis-
discussed below. These operations normally are conducted with other elements such as military police (MP), combat troops, civil affairs and psychological operations teams, and they require close coordination and joint planning.

b. Counterintelligence Screening. Refugee and prisoner of war screening by counterintelligence personnel is conducted with the view to intercepting hostile intelligence agents, saboteurs, and subversives trying to infiltrate friendly lines.

(1) Coordination. Planning for these screening operations is accomplished, as far as possible, in conjunction with the following elements:

(a) Combat commander. The commander is concerned with channelizing refugees and prisoners of war through his area of operations, particularly in the attack, to prevent any impediments to his unit's movement, or any adverse effect on the unit's mission.

(b) Military Police (MP). MP elements are responsible for the control and evacuation of prisoners of war and refugees through the different echelons.

(c) Civil Affairs (CA). CA elements, under the G5, are responsible for the proper disposition of refugees and prisoners of war.

(d) Psychological Operations (PSYOP). PSYOP elements, under the G5, contribute to screening operations by informing the refugees of the need for their displacement. They also assist the MP in maintaining control.

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

(2) Preparation.

(a) Before any screening operation, the CI teams involved should become intimately familiar with all available information on indicators as covered in paragraph 12-11e, as well as the following:

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

2. Enemy intelligence, political infrastructure and organizations. In order to identify agents of the enemy intelligence or infrastructure apparatus, CI personnel must be thoroughly conversant with their methods of operation, policies, objectives, offices and suboffices, schools, officials, and known agents.

3. Enemy order-of-battle (OB). Every member of the CI team should know which units of the enemy his unit is facing and which units are in its area of operations. He should be aware of their disposition, strength, weaknesses, composition, training, equipment, activities, history, personalities, and commanders. Current OB information should be maintained by the team for possible exploitation of prisoners of war and for assistance to OB analysts. Counterintelligence personnel are not OB interrogators but they must be capable of expeditiously recognizing, detecting, exploiting and reporting tactical and OB data.

4. Enemy-held area. CI personnel should also become familiar with the area in which they are operating; particularly geography, landmarks, distances, and travel conditions. Knowledge of such pertinent information as the political, social and economic traditions, customs and racial problems of the area is essential.

(b) Black lists and information sheets listing indicators of CI interest should be distributed to the troops, MP, or other personnel assisting with the screening operation. A form should be made up and passed 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 EEI or OIR. The following data, plus anything else deemed pertinent, should be included on the form:

1. Full name, other names, date and place of birth, current and permanent residences, and current citizenship of the individual.

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

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

4. The individual's education and knowledge of languages.

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

6. Point of departure, destination and purpose.
(3) Initial screening. Prisoners of war and refugees enter prisoner of war and refugee streams rearward at the forward edge of the battle area (FEBA) where the troops channelize them after a search for weapons and documents. (Fig 12-1 depicts the prisoner of war and refugee flow.) Couriers, walking wounded, and empty trucks or convoys traveling rearward toward the brigade control points can be used as guards and/or transport for the prisoners of war and refugees. At this point MP will take custody and responsibility for the prisoners of war and refugees, and initial CI screening will take place. This will consist of, as a minimum, interrogation by intelligence interrogation personnel. These personnel will refer suspects to the CI team for further interrogations and possible detention. At this level, suspects are separated from the prisoner of war and refugee streams, exploited if possible, and evacuated to division by MP. Detained prisoners of war and refugees will be interrogated, further exploited at division prisoner of war collecting points or civilian detention centers, and then evacuated to field army civilian detention centers or prisoner of war cages for detailed interrogation and exploitation, if applicable. Those refugees found to be innocent of any wrongdoing will be rerouted to the civilian assembly areas. Those prisoners of war and refugees not detained will follow the refugee flow to the division control points where more detailed CI screening is conducted similar to that system at brigade. Those not detained will be collected and routed to the field army civilian assembly area or prisoner of war cage.

(4) Conduct of screening. Since it is impossible to interrogate everyone because of time and the usually large number of people to be interrogated, 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. These selected persons are detained for further CI interrogation. If the interrogee is to be referred to a rear echelon for the detailed interrogation, a preliminary interrogation report (PIR) is furnished the MP who accompanies the interrogee to the rear. The MP will take both the detainee and the PIR to the next echelon CI team. The mechanics of this referral procedure will be a matter of operational orientation. Personnel who conduct the detailed interrogations at rear area interrogation centers will not be the same as those who conduct the preliminary or screening interrogations. The PIR, therefore, should reflect as much data as possible under these four headings:

(a) Identity. Persons should be searched for possible identifying documents in the form of ID cards, ration cards, draft cards, driver's license, auto registration, travel documents, passport, and the like. If a man is, or has been, a soldier, his rank, service number, and unit should be recorded. All this information can be checked against the form previously filled out by the interrogee.

(b) Background. The use of the form will aid in obtaining the information required; however, certain informational areas on the forms will have to be clarified, especially if data indicate a suspect category or the person's knowledgeable of intelligence information.

(c) Recent activities. The activities of an individual during the days prior to his detention or capture should be examined. What was he doing to make a living? What connection, if any, has he had with the enemy? Why was he in the area? This line of questioning may bring out particular skills such as those associated with a radio operator, linguist, photographer, etc. Physical checks can be made of certain types of callouses, bruises, or stains to corroborate or disprove his story. Sometimes soil on shoes will not match that from the area he claims to have come from.

(d) Journey or escape route. CI personnel should determine the route the individual took to get to US lines or the checkpoint. The individual should be further questioned closely on time, distance, and method of travel so that the screener will be allowed the opportunity to quickly calculate whether or not the trip was feasible during the period of 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 whose cover story is very shallow. By ascertaining what an individual observed en route, the screener can either check the person's story or pick up intelligence information concerning the enemy forces.

(5) Indicators. The following indicators can be used in an attempt to identify hostile infiltrators.

(a) Persons of military age.
(b) Persons traveling alone or in pairs.
(c) Persons without identification.
(d) Persons with unusual documents.
Figure 12-1. Channelizing of prisoners of war and refugees.
(e) Persons possessing large amounts of money, precious metals, or gems.
(f) Persons displaying any peculiar activity.
(g) Persons trying to avoid detection or questioning.
(h) Persons using enemy MO.
(i) Persons having a pro-enemy background.
(j) Persons with a suspicious story.
(k) Persons with a family in enemy areas.
(l) Persons with a technical skill or special knowledge.
(m) Persons who have collaborated.
(n) Persons who violate regulations in enemy areas.

(6) Other screening methods. In addition to interrogation, the following methods of screening prisoners of war and refugees can be used.
(a) Black, grey, and white lists.
(b) Low-level informants inserted into the prisoner of war or refugee screens, cages, or centers.
(c) Sound equipment placed in suspect holding areas or cages.
(d) Polygraph examinations.
(e) Specialized identification equipment, e.g., metal-trace detection kit.

(c. Mobile and Static Checkpoints. This type of CI screening requires that counterintelligence personnel prepare black and grey lists, indicators, and some specialized equipment such as metal detection kits to be used by screening teams. These teams will provide the initial screening and will detain and refer suspects to the MI control element for detailed interrogation and possible exploitation.

(1) Screening teams can be made up of combat troops, military police, civil affairs, intelligence interrogators, counterintelligence agents, or any mix thereof.

(2) Checkpoints are placed at strategic locations where there is sufficient space for assembling people under guard and for parking vehicles for search and investigation and are set up ideally as shown in figure 12-2 as either mobile or static missions. Local security must be posted to protect the checkpoint and a sufficient amount of personnel must also be posted to the front and rear to apprehend anyone attempting to avoid the checkpoint.

(a) A mobile checkpoint can be used as a moving system whereby the team, either mounted or on foot, briefly selects individuals at random or systematically, e.g., every fifth person, to be stopped and questioned. These checkpoints could be located at various points for periods not to exceed 1 day.
(b) Static checkpoints are those manned permanently by MP or troops at the entrance to a brigade, town gate, river crossing, or similar strategic point.

(3) Mobile and static checkpoints are used by counterintelligence to:
(a) Detect and prevent enemy infiltration of espionage, sabotage, or subversive agents into the area.
(b) Gather information of immediate intelligence value, both tactical and counterintelligence, from refugees and other persons from enemy-controlled areas.
(c) Gather other information not otherwise available to intelligence units.

(4) The preparation needed for static and mobile checkpoints is identical to other screening operations, and the indicators will remain basically the same.

d. Port and Harbor Security. Port and harbor security normally is conducted jointly between the MP and MI units assigned to the logistical command under which the port is operated. Counterintelligence elements normally will concentrate their efforts in the following areas:

(1) Special operations. Those special operations described in FM 30-17A, the classified supplement to this manual, will be targeted against the surrounding and internal areas with special emphasis on hostile sabotage and subversion elements.

(2) Physical security. Normal CI procedures will be established for port and harbor areas as are set forth for installations, except that controls must also be established for ships and crews in port, particularly those under a foreign flag.

e. Border Security. Border Security is conducted by CI element to minimize infiltration of men and supplies into the area of operations—particularly hostile intelligence or elements which will engage in sabotage and subversive activities against the friendly war effort. To accomplish this, CI elements must determine hostile methods of operation to establish indicators and must determine infiltration and exfiltration points to successfully capture or neutralize infiltration. The indicators will be furnished those friendly elements in contact with the border areas, and to
Figure 12-2. Checkpoint.

LEGEND:

- Concealed elements which seize personnel who attempt to turn back.
- Security elements.
- Vehicle and personnel inspection areas.
other MI elements. In addition the friendly military forces, to include MP and CA elements, may utilize those indicators received from the interception of radio communications when conducting border surveillance and making documentation checks at mobile and static checkpoints (c) above). Other MI units can make use of the indicators when engaged in aerial surveillance or image interpretation missions. Information thus received can go into planning for neutralization and exploitation operations, or use of detection powders at possible infiltration points as well as interrogation of border area residents and travelers.
CHAPTER 13
STABILITY OPERATIONS

Section I. INTRODUCTION

13–1. General

a. To fully understand the counterintelligence problems and the application of counterintelligence techniques and procedures in stability operations, counterintelligence personnel must be thoroughly acquainted with insurgency, its causes and characteristics, and the peculiarities of US Forces employment in insurgency areas. FM 30–31, FM 30–31A, and FM 31–23 should be studied as background for the issues covered here.

b. The normal counterintelligence functions of routine security investigations and services are performed in much the same way as they are in a conventional tactical situation. The basic responsibilities of CI elements and personnel in an insurgency area are the denial of intelligence information to the insurgent force and the identification and neutralization of the insurgent infrastructure. Particular emphasis should be placed upon the intelligence apparatus. Counterintelligence operations must not only provide security against espionage, subversion, sabotage, and terrorism, but they must include the collection of information on the insurgents, their organizations, and their activities. Detailed information on the insurgent intelligence apparatus, methods of operation, targets, and capabilities is required as a basis for CI planning and the conduct of an effective security program. In addition, this planning can be used for future tactical missions by combat units to neutralize CI targets.

c. If the insurgency is dominated by a Communist regime, a study of the political apparatus must also be made since the philosophy that the military exists only as an extension of the political arm, and is subordinate to it, will dominate the insurgency. Such a study, if it is continuous, may yield information more revealing than a study of only the military aspects of an insurgency or it may become the key to future operations, missions, or goals set for the military by the overriding consideration set by the political arm. A discussion of such a study is contained in FM 30–17A, the classified supplement to the manual.

d. To accomplish security objectives, the CI effort in the following areas must be stressed:

(1) Denial of all information (classified or otherwise) to the insurgents by devising security controls to prevent breaches.

(2) Formulating and planning security training programs and implementing security controls.

(3) Detection, investigation, and elimination of security breaches and weaknesses.

(4) Detection, identification, and neutralization or destruction of hostile intelligence, subversive, sabotage, and terrorist elements and activities.

(5) Monitoring the populace and activities in the area of operation for indications of threats to the security of US/host country activities.

e. The police, in the course of investigating crimes and conducting police law and order operations, may be the first government agency to detect evidence of an insurgency. Police intelligence can provide significant information through MI channels and command intelligence for counterinsurgency operations. Intelligence collection guidelines for police and MI agencies should be exchanged in the preconflict environment of the first phase of an insurgent threat to assure the timely provision of police intelligence to MI and CI agencies and civil intelligence agencies responsible for detection, surveillance, and penetration of insurgent organizations.

13–2. Jurisdiction and Responsibility
Counterintelligence measures normally will have been carried out by agencies of the host country prior to arrival of US Forces in the country.
Army CI elements, as part of the US Forces, will arrive in the host country by request or invitation. Counterintelligence activities of US personnel may be limited to training, advising, and supporting the host country counterintelligence and security services. However, with the participation of US Forces in stability operations, the normal CI support of these forces must be provided.

Section II. COUNTERINTELLIGENCE OPERATIONS


Personnel security investigations will be conducted in accordance with this manual and AR 381–130. Security investigations of local nationals involve additional problems.

a. Subjects may be from Communist- or insurgent-controlled areas, within or outside the host country, where investigation cannot be conducted. Special notice must be taken of a subject's listed residences to determine if they were or are in insurgent-controlled areas.

b. There may be an absence of reliable and current records of all types, particularly in newly emerging nations, thus reducing the effectiveness of background investigation.

c. In most instances, host country intelligence and security agencies, which may be penetrated by the insurgents, will be responsible for investigating and clearing local personnel; capabilities of local agencies will vary from excellent to nonexistent.

d. The volume of clearance actions on local nationals (military, cooks, maids, drivers, interpreters, laborers) who have frequent access to US installations and the probability of limited personnel for conducting background investigations may dictate the necessity for limiting the scope of investigations. Employment of local nationals is discouraged for security reasons, and, when necessary, should be kept to a minimum. Under these conditions, steps may be taken to prevent undue risk. One step is to obtain the specific indorsement of the loyalty of a subject by persons whose loyalty and reliability have already been established (the “guarantor system”).

13—4. Security of Information

a. US Army activities involve daily contact with host country personnel over whom US Forces exercise no security control. This unavoidable security risk must be balanced with strict security discipline and effective application of basic principles of safeguarding military information.

b. The difficulty in distinguishing between friendly and insurgent elements among the host country populace magnifies the problem of “loose talk.” Loose and careless discussion of unclassified military information presents an even greater problem inasmuch as the absence of a security classification gives free license to discussion. Such unclassified bits of information in the hands of insurgents lead to ambushes, surprise raids, and acts of terrorism. The security training and education of troops must stress that disclosure of unclassified information may be as dangerously detrimental as disclosure of classified information. The indigenous employees of US Forces facilitate the insurgent’s acquisition of information on our activities, both military and personal.

c. Measures which screen the staging, grouping, training for, and planning of military actions from the observation of the insurgents and the population are extremely important. Troops must be warned against patterns of conduct which reveal the tactical intentions of their units. They must be reminded that the populace is the primary source of intelligence information for the insurgents. Counterintelligence personnel must learn to distinguish what patterns of conduct are used by the insurgent as indicators and rapidly report these indicators to the responsible command.

13—5. Physical Security

a. The effective protection of military installations, personnel, and activities from the threat of espionage and sabotage is based on security measures implemented and practiced as a result of CI surveys and inspections and the physical security surveys conducted by the MP. Counterintelligence surveys provide recommendations on security measures designed to fit specific installations, facilities, or activities. A checklist for conducting CI surveys is contained in appendix D. A checklist for conducting physical security surveys is contained in FM 19–30. In all surveys, particular emphasis should be given to a check of:

(1) The natural topographic features existing at the periphery of the installation to deter-
mine whether they afford direct observation into the installation, afford a concealed or covered path of approach into the installation, or otherwise adversely affect the security of the installation.

(2) Organizations (political, labor, fraternal, social) in the area which may present a security threat.

(3) Places of entertainment (bars, restaurants, night clubs) in proximity of the installation to determine whether there have been or may be attempts to solicit information from the soldiers.

b. Periodic CI inspections must be conducted at great frequency in an insurgency environment. Close attention must be given to:

(1) Close examination of the defensive system to insure that every possible means of access or path of approach has been considered in establishing the physical perimeter security. Particular attention must be given to culverts, gulleys, and streambeds which could provide means of access to guarded areas.

(2) Designation of all sensitive areas of the installation as restricted areas and posting of "off-limits" signs in both English and the local language. Access to restricted areas by local hire personnel such as janitors, cooks, guards, translators, and clerks should be prohibited or permitted only when properly escorted by authorized personnel. It may be advisable to conduct periodic technical inspections of restricted areas to preclude or detect the presence of electronic listening devices which may be planted by opposition elements. Additionally, the periodic shifting of key installation locations, e.g., command post, radio room, will aid overall security.

(3) A strict visitor control system for handling the constant security threat posed by the presence of laborers, local tradesmen, and relatives of camp personnel. Security considerations may dictate making the entire base area a restricted area into which no civilians are allowed. Laborers should be closely checked and prevented from loitering near sensitive areas.

(4) The location of sanitary fills, washing areas, and other troop-associated facilities. Whenever possible, such facilities should be within the cantonment.

c. A unit security SOP must be prepared at all echelons, and all members of the unit must be familiar with established security procedures and practices. As a minimum, a security SOP must provide for:

(1) Duty details for emergency conditions.

(2) Immediate availability of adequate weapons and munitions for immediate defense of the installation.

(3) An installation warning system to sound the alert.

(4) Defense plans indicating posts for all members in the event of an assault, and a fire plan for all weapons.

(5) Liaison with local security organizations and tactical units to provide support in case of attack, to include such items as a prearranged fire support plan by artillery elements.

(6) Emergency destruction plan for defense information and equipment.

(7) Security discipline and standards of conduct to be observed.

(8) Duties of security guards and patrol arrangements indicating frequent changes of timing and methods of patrolling, location of guard posts, and changing of the guards. No discernible pattern in time or method should be established.

d. All security measures should be viewed and undertaken with the knowledge that in stability operations there is no rear area; the enemy is on all sides.

13-6. Populace and Resources Control

a. A significant factor in stability operations is the implementation of measures to watch and control the movement channels and patterns necessary for support, communication, and operations of insurgent forces. Prior to implementation of any control measures, a public information program must be initiated to inform the population of the reason for the controls. Imposition of excessive or unnecessary restrictions on movement will result in the buildup of a strong resistance from the people and should be avoided. To the maximum extent possible, populace and resources control should be implemented and performed by host country agencies. This is a matter of practicality, but there are also legal and psychological implications. US Army counterintelligence specialists should participate in the planning stage of a populace and resources control program and provide advice and assistance to the host country.

b. Some examples of populace control techniques are:

(1) Nation-wide registry and issuance of identification cards to all residents and supplemental family registration program.
(2) Division of communities or areas into blocks with appointed, trusted, and loyal residents as block leaders to report on insurgent activities.

(3) Use of police patrols to detect sources of insurgent support, insurgent sympathizers, and routes used by insurgents.

(4) Establishment of checkpoints to screen and control movement of individuals into and out of zones of operation or other specified areas.

(5) Employment of travel restrictions to detect violators and nonlocal residents; frequent change of restrictions and travel bans at certain hours of the day.

(6) A well regulated and controlled curfew should be employed during hours of darkness to reduce terrorist and sapper attacks.

(7) Censorship.

(8) Prevention of illegal political meetings and rallies.

(9) Search operations are conducted to clear a built-up area, search watercraft, apprehend guerrillas, and seize illegal arms, communication means, medicines, and other items of a critical nature. A search operation is conducted as a preventive measure against the accumulation of critical items by the population, the harboring of insurgents, and in accomplishing administrative control measures previously established.

(10) Block control (para h below).

c. Some examples of resources control techniques are:

(1) Control of production, storage, and distribution of foodstuffs, and protection of food-producing areas.

(2) Control of the possession of arms, ammunition, demolitions, drugs, medicine, and money.

(3) Decreeing the possession of such chemical combinations as arsenic sulfate and potassium chlorate, which create explosives, as illegal without a special permit.

(4) Control of certain imports, e.g., 82mm pipe which can be converted into mortars while permitting import of other pipes, i.e., 77mm construction pipe.

d. In stability operations, border or frontier control must be an integral part of the populace and resources control program. Border control measures can prevent or impede the movement of insurgents into a bordering country for sanctuary and also restrict materiel and manpower support to the insurgents. Prior to implementation of control measures, a thorough study and analysis is made of the terrain, vegetation, and human environment along the border areas. Factors to consider are the activities, intents, and haunts of border residents, illegal border crossers, and smugglers and the locations of natural geographic features which are impediments to human travel.

e. Of primary concern to CI elements involved in border or frontier control during stability operations is the infiltration of hostile sabotage, espionage, and subversive elements into and out of the host country. This infiltration can be by sea, land or air. These routes must be detected and neutralized. The following EEI frequently will be standard in border or frontier control:

(1) Infiltration-point locations.

(2) Exfiltration-point locations.

(3) Methods of operation.

(4) Indicators of hostile infiltration/exfiltration.

f. In planning for implementation of a border control operation, the following points should be covered:

(1) Location of authorized road and rail crossing points along the frontier.

(2) Establishment of frontier control points to determine identities of persons attempting to enter or leave and to check their documents.

(3) Provision to apprehend anyone attempting to evade control restrictions.

(4) Control of frontier area residents.

(5) Provisions for interrogation and disposition of apprehended suspects.

(6) Security control of refugees and displaced persons attempting to cross the frontier.

(7) Liaison with border control authorities of neighboring countries, if they are friendly.

(8) Mobile and static checkpoints.

(9) Neutralization and exploitation operations.

(10) Travel permits.

(11) Documentation checks.

(12) Imagery interpretation reports on possible infiltration/exfiltration points.

(13) Restricted zones enforced by air strikes/artillery fires.
(14) Detection powders laid on possible infiltration points.

(15) Surveillance, to include use of illumination, radars, night vision devices, and ground sensors.

(16) Special operations, as discussed in FM 30–17A.

(17) Other intelligence, as acquired.

g. Resources control measures are necessary to impede or prevent the flow of food, supplies, and materiel to the insurgents. Insurgents are dependent primarily upon the local populace for logistical support; therefore, regulatory or restrictive measures (rationing of critical supplies) to preclude surpluses will affect the availability of these items of the insurgent. Planning must include provision for disposal of scraps, waste, and unserviceable equipment and supplies to prevent utilization by the insurgents.

h. Block control is the constant surveillance and reporting of activities within a block or other small, populated area by a resident who has been appointed and is supervised by an appropriate authority in the host country. Block control is one of the most effective and economical means of populace and resources control; however, the system takes considerable time to establish and, by its nature, operates more effectively under civil authority than under military control.

(1) Block control is instituted by dividing each block (or area) in zones, each of which includes all the buildings on one side of a street within a block. A zone leader is appointed from among the residents for each zone, and a separate block leader is appointed for each block. Zone leaders report to block leaders all movements, to include arrivals and departures. The block leader reports periodically to the military commander or civil authority on all movements within his block. Unusual activities are reported immediately.

(2) If the loyalty of the zone and block leaders is questionable, informants may be located throughout the area as an effective check on their operations.

13–7. Special Operations
Counterintelligence special operations in stability operations are discussed in the supplement to this manual, FM 30–17A, and in FM 30–31A.

Section III. OPERATIONAL TECHNIQUES AND PROCEDURES

13–8. General
The basic CI techniques and procedures discussed in this manual and its supplement, FM 30–17A, are generally applicable in an insurgency environment. Requirements for highly technical investigatory equipment are less than normal. Some modifications or adaptations of techniques and procedures are necessary.

13–9. Counterintelligence Coverage
In stability operations, CI coverage resembles that coverage as described in chapter 12, Conventional Combat Operations, in that area and tactical coverage is again used. The differences will be that tactical MI companies are responsible for that area of influence around its tactical area of responsibility (TAOR). Area coverage will overlap the TAOR primarily for strategic type coverage. Normally, too, CI elements will not have any investigative jurisdiction over indigenous civilians or US citizens in the supported nation. The area coverage elements normally will be given advisory duties in addition to the normal mission of area coverage.

13–10. Base Camp or Installation Security
Base camp or installation security in stability operations should involve defensive and offensive measures. Since defensive measures alone will tend to play into the insurgent's strategy, the initiative is usually the enemy's in an insurgency, therefore, both types must be employed. Some of these measures can be taken from paragraph 12–5, which pertains to rear area security in a conventional war situation, but others and either not mentioned in detail or are conducted differently in an insurgency.

a. Defensive Measures. In conjunction with other agencies, primarily the MPs, the five basic areas of base camp or installation defense are those concerned with physical security as listed below.

(1) Security forces. Counterintelligence interest in the security forces of an installation, compound or activity is the proper clearance of indigenous employees.

(2) Detection measures. While this area is basically an MP responsibility, since it involves
the use and deployment of sentry dogs, night vision devices, anti-intrusion devices, and alarm systems to list a few, counterintelligence personnel qualified in the DAME, DASE, and photographic specialties can be of assistance to any MP element without this specialized training.

(3) Internal security measures. Counterintelligence must assume the greater responsibility for education in the area of internal security measures. SAEDA lectures in conjunction with MP classes on other aspects of security such as fire prevention, arms control, and safety, will take up most of this aspect of physical security.

(4) Perimeter measures. A prime MP area, perimeter measures consists of advice to the commander on such things as outer perimeter patrolling, barriers, protective lighting, and clear zone. Counterintelligence and police intelligence informant nets near and within the activity, when properly integrated, will also be needed for proper protection of the installation.

(5) Control measures. This widely overlapping area is shared by counterintelligence with the MP element, and includes such measures as population control in and around the activity; vehicular, personnel and package control into the activity; and restricted areas.

b. Offensive Measures. The primary objective should be the identification and neutralization of specific members of the insurgent infrastructure through systematic intelligence collection and analysis with complete documentation concerning the activities of each individual. The ultimate objective being to allow the host country to prove the individual's illegal activity once he is apprehended. This will require that CI personnel work very closely with host country agencies. Liaison and exchange of information with the area coordination centers, if they have been established; or with the civilian police, military and civilian intelligence agencies in absolutely necessary to insure that offensive CI measures are completely effective. Since the host country agencies will have the prime responsibility for identification and neutralization of the infrastructure, US CI activities should complement those of the host country. CI personnel should be the focal point for exchange of information concerning the infrastructure, between the US units and host country organizations.

(1) HUMINT, as discussed in FM 30-17A and FM 30-31A should be used offensively.

(2) Mobile checkpoints as discussed in paragraphs 12-15 and 12-16 is a type of offensive CI measure.

(3) Cordon and search operations.

(a) General. In stability operations, cordon and search operations may be employed to ferret out the insurgent infrastructure as well as individual unit elements which may use a community or area as cover for their activities and/or as a support base. These operations should be conducted in conjunction with host country forces and organizations, not as unilateral US efforts. Ideally US Forces, to include CI personnel, should provide support and the entire operation should be directed by a host country official. Host country personnel should, as a minimum, be part of the screening and sweep elements on any cordon and search operation.

(b) Preparation. Before conducting a community or area cordon and search operation, counterintelligence personnel must:

1. Coordinate with local officials to solicit their support and cooperation in the operation.
2. Coordinate with the host country area coordination center, if established, or if not, the host country intelligence and police organizations: To obtain their participation in the operation; to update existing black and gray lists; to arrange to have insurgent defectors, agents, and other knowledgeable personnel present to identify insurgents and their supporters; to update all intelligence on the community or area.
3. Coordinate with US and host country CA and psychological warfare teams for entertainment and civic services.
4. Coordinate with the unit commanders who will be involved in the operation for details on the conduct of the operations.
5. Update all intelligence on the community or area.

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

1. The basic operation is the community cordon and search operation (fig 13-1). As the collection/screening station (fig 13-2) is set up by the screening element, the sweep element escorts the residents toward the collection/screening station, leaving behind one resident to care for family belongings, if required by law. The search ele-
ment follows behind the sweep element searching houses, storage areas, cemeteries, etc., with dogs and metal detection equipment, if available. Each search element should include an interrogator with a blacklist to screen persons left behind to watch family belongings. In the collection/screening station, the residents are brought to the collection area (or holding area) and then systematically led to specific screening stations. En route to the screening station, each individual will be searched for weapons and will pass by the mayor or community leader, enemy defectors or cooperating prisoners hidden from view so that they can uncompromisingly identify any immediately recognizable enemy. These informants will be provided with a means by which to notify a nearby guard or a screener of the spotted enemy member who will be immediately segregated and interrogated. At the specific screening stations the residents will be asked for identification, checked against blacklists, searched for incriminating evidence or "body-marks" or, if available, checked by electronic equipment. If found suspect or guilty of enemy activity, persons are moved on for photographing, further interrogation or put in the screening area detection point to be taken back to a base area or area coordination center interrogation fa-

Figure 13-1. Community cordon and search.
Figure 13-2. Collection/screening station.
ility for detailed interrogation upon completion of the operation. Innocent residents are passed through to the post screening area where they are provided medical assistance and other civic assistance, as well as entertainment and friendly propaganda. Any persons caught attempting to escape or break through the cordon are immediately returned to the detention area. When the operation is terminated, all innocent individuals are allowed to return to their homes and the enemy suspects are removed under guard for further interrogation. All members of the community will be photographed for compilation of a village packet, (see FM 30-17A) which will be used in future operations.

2. 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, towns, or villages which are subdivisions of a political area beneath county level. 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. It will generally appear as illustrated in figure 13-3. While screening and search teams systematically go from community to community within the area 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, counterintelligence agents will insure documents testifying to the fact that he was screened and, if necessary, allowing him restricted travel within the area. Other population and resources control measures are used as well, and such an opportunity may allow the chance to issue new ID cards and photograph all of each hamlet's residents. As each community screening proceeds, individuals who were designated for further interrogation are sent to an interrogation center set up at a centralized point in the cordoned area where CI personnel will work with intelligence interrogation personnel, both US and indigenous, and with police and other security service interrogators. Besides field files and other expedient facilities, located at the interrogation center is a quick reaction force ready to react immediately to intelligence developed during the interrogations and from informants planted among detainees.


a. The language communication barrier in most nations with potential insurgency is a major handicap to CI operations. The employment of indigenous personnel with English language ability will be essential. These persons will serve not only as interpreters but as intermediaries in contacting and developing sources of information. To minimize the security risks involved in employment of indigenous personnel, the following precautionary measures must be considered:

(1) Employment of indigenous personnel who are members of the host country military or police services.

(2) Quartering and messing of indigenous employees within the US base area for purposes of activity and movement control.

(3) Use of polygraph examination for initial pre-employment check and periodic re-examination.

b. In many cases, it will be difficult to find enough indigenous personnel who are proficient in the English language. To avoid misunderstanding or misinterpretation caused by limited language proficiency, US counterintelligence personnel and indigenous personnel must work as teams with the US personnel providing the professional guidance and direction. Reports from indigenous personnel must be closely scrutinized for reliability and accuracy of content. Obscure points must be questioned to insure accuracy. Sociological factors must be considered to determine the extent to which ties of blood, race, language, locality, religion, or tradition may affect the substance of translated information.

13-12. Pattern Analysis

A discussion on methods of pattern analysis on insurgent groups is contained in FM 30-17A, the classified supplement to this manual.

13-13. Records and Files

a. Principal sources of information for counterintelligence personnel in stability operations are
Figure 13-3. Area cordon and search.
the documents and records maintained by the host government offices and civilian organizations. One of the initial tasks of counterintelligence personnel in an insurgency area is locating, gaining access to, and establishing continuing access to the documentary sources available. Generally, the records maintained in the newly emerging countries are more limited and much less reliable than those in longer-established nations.

b. Some of the more important types of records pertinent to CI operations are:

(1) Police and security agency records. Counterintelligence personnel must become thoroughly familiar with the local records systems to insure that all pertinent files are checked in each instance.

(2) Intelligence agency records. In many newly emerging nations, intelligence capabilities and operations are limited or confined to activities which are primarily political in nature. Utilization of US intelligence personnel with fluency in the local language and having a related ethnic background is highly desirable.

(3) Residence or family records. Normally these records are maintained by local police stations.

(4) Immigration and travel records. Such records may be incomplete, but they are of value to CI operations.

(5) Political and Religious Sources. Political organizations and religious sects, particularly in newly developing countries, will often operate intelligence networks for their benefit. At times, a third country, such as the US, may be allowed access to information from these networks. Such information, particularly on the insurgent, may be very accurate, but it must always be viewed as suspect since that organization may slant the information for its furtherment.

(6) Miscellaneous organizational records. Membership lists may be available.

c. Efficient and effective CI operations require the establishment and maintenance of a complete system of files and records on all known or suspected sympathizers of the insurgency movement. Variant spellings of local names must be cross-referenced.

13-14. Use of Standard Procedures and Techniques

Experience indicates that the procedures and techniques outlined in this manual are generally effective in all types of situations and environments when used appropriately and with common sense. Every attempt must be made to use these procedures and techniques, adapting or modifying them when the situation so demands. Conversely, the development of new techniques should be reported expeditiously (para 1-1e) to permit appropriate expansion of doctrine.
CHAPTER 14
INTERRELATIONSHIPS

Section I. INTRODUCTION

14—1. General

a. In conventional combat operations, and especially in stability operations, CI elements must maintain particularly close coordination and liaison with civil affairs (CA), psychological operations (PSYOP), and military police (MP) elements, as well as other friendly agencies in the area of operations. In many cases CI elements work with those elements in joint operations to support the combat commander.

b. Assistance is, as a rule, a two-way street; CI elements can provide CA, PSYOP, and MP elements with information and assistance and they, in turn, can often furnish the same to CI elements.

Section II. RELATIONSHIP WITH CIVIL AFFAIRS

14—2. General

A close working relationship and continuous coordination between CA and CI units/elements are necessary at all levels of operation to provide for an exchange of information between the agencies.

14—3. Coordination Procedures

Policies for coordinating CA and MI efforts should be developed at the general staff level. Once policy is developed and coordinated, it should be promulgated in writing to all affected units to familiarize both MI and CA personnel with each other’s operations and responsibilities.

14—4. Loyalties of Indigenous Personnel

a. Counterintelligence and CA elements have a concurrent requirement to determine the loyalty of local officials in a conventional war situation in cases where agreements have not been made between nations. This should be a continuously coordinated effort with mutual responsibilities and objectives. In stability or mid-intensity operations this requirement may be modified by agreements such as a formal status of forces agreement. The control office, usually G2, will determine the scope of the CI investigation to be performed or adhered to by third country investigative bodies in cases where the US retains the right to reject employees who do not meet specified criteria.

b. In a conventional war situation background investigations of indigenous labor personnel are considered a standard operational procedure and a CA requirement. Counterintelligence units, because of their mission, are responsible for security investigations. Civil affairs operations require background investigations of a broad nature to determine suitability of indigenous personnel for positions of trust and responsibility or public association with US or allied military government. The objective of the background investigations is to minimize subversive and hostile infiltration into official or important positions through which the mission of the US Army would be hindered.

c. In stability operations, identification of the insurgent subversion and infrastructure apparatus is a high priority target for the CA intelligence effort which has as its primary goal the reestablishment of civil order within the troubled country.

14—5. Attitudes of Indigenous Personnel

Attitudes of the indigenous population toward US troops is a primary area of concern, since CA operations are developed to create or exploit local attitudes. If this information is available to CA elements, it will assist CI elements in the assessment of the area for CI operations. If this information is not available to CA elements, CI can be of assistance if it is well established in the area.
Counterintelligence elements must continuously monitor the populace for any changing attitudes that may be influenced through enemy coercion and subversive efforts. They must also work with CA on programs designed to counter and neutralize any hostile threat. In the early stages of an insurgency, CI will orient its monitoring mission primarily on subversion, but this emphasis will gradually be reoriented toward espionage and sabotage if the insurgency moves into phases II and III.

14—6. Procurement and Recruitment

Direct support to intelligence collection agencies may be provided by CA units in the procurement of essential facilities and equipment and the recruitment of personnel.

a. Procurement. In addition to normal CA procurement, CA personnel may also procure:

(1) Biographical data on key persons in the civilian community or other identifying information essential to special operations.

(2) Civilian clothing and items of normal personal possession.

(3) Maps.

(4) Civilian equipment such as binoculars, cameras, recording devices, and radios.

(5) Documentary matter including passports, visas, vehicle operator licenses, birth and marriage records.

(6) Indigenous funds.

(7) Foodstuffs, tobacco products, or alcoholic beverages peculiar to the area.

(8) MEDCAP teams, water trailers, and like facilities to support cordon and search operations in stability operations.

(9) Barter items.

(10) Civilian motor vehicles, bicycles, or domestic animals.

b. Recruitment. Through contact with civilian organizations, leaders, and political enemies of hostile governments, CA personnel can compile personnel rosters or spot possible enemy infiltrators for screening by CI or PSYOP personnel for use as:

(1) Interpreters.

(2) Informants.

(3) Counterintelligence special operations operatives.

(4) Specialized craftsmen, technicians, or laborers.

14—7. Civil Security

a. CA units provide maximum support to CI elements in the detection and prevention of espionage, sabotage, subversion, guerrilla aid, and in other similar activities including the following:

(1) Identification of known or suspected hostile agents, collaborators, or sympathizers.

(2) Prevention of local publication of information or opinions which are inimical to the military force.

(3) Control of credit, foodstuffs, clothing, medical supplies, and related items which may be used to support guerrilla activities.

(4) House-to-house searches for contraband which may yield persons, documents, or materiel of CI interest.

(5) Seizure and impounding of mail pending instructions for screening and disposition.

(6) Conduct of searches for documents of intelligence interest.

(7) Placement of administrative surveillance and restrictions on the movement of persons suspected of collaborating with guerrilla forces.

(8) Destruction, surveillance, or control of potential hiding places or shelter spots of dissidents, such as abandoned mines, caves, isolated rural buildings, haystacks or similar crop collections.

(9) Collection, evaluation, and interpretation of police statistics relating to insurgency crimes, such as the recurrence of acts of terrorism, which may relate to enemy sabotage, espionage, or subversive activities.

b. While the close contacts and working relationships between personnel from CA units and the civilian population provide valuable intelligence sources and material, CA units have a two-way potential since they not only serve friendly forces, but may provide an opportunity for exploitation by unfriendly persons and groups. CA personnel must be particularly discreet in their dealings with the civilian population. Information provided civilians should be carefully screened, and indigenous persons and agencies should be kept under continuing surveillance for indications of disaffection.
14–8. Collection Potential of CA Personnel

Civil affairs personnel in their day-by-day operations deal with people, equipment, and documentary matter, all of which are primary sources of information of intelligence value. Normally, when persons with information of possible value are discovered, they are referred promptly to appropriate intelligence personnel for exploitation. Those sources CA personnel are likely to locate include:

a. Refugees, evacuees, and displaced persons who may be interned or otherwise come under CA control or sponsorship.

b. Civilians who were associated with enemy personnel.

c. Political enemies of the hostile regime.

d. Leaders of fraternal, civic, religious, or patriotic organizations.

e. Governmental documents, libraries, or archives.

f. Files of newspapers or periodicals.

g. Industrial and commercial records.

h. Persons employed in recreational areas.

i. Political prisoners of the hostile regime.

j. Technical equipment, blueprints, or plans.

14–9. Other Civil Affairs Assistance

Other supporting activities in which CA personnel can make significant contributions to the CI effort include:

a. Collection of all types of intelligence information for use at different levels of command.

b. Procurement.

c. Recruitment.

d. Assistance to counterintelligence personnel in the following activities:

   (1) Screening civilian officials.

   (2) Obtaining information pertaining to sabotage.

   (3) Detecting the transmission of information and supplies to enemy forces, unfriendly partisans, or guerrillas through audits of supplies in warehouses, audits of controlled merchandise in stores, illegal activities, and routes of communications.

   (4) Locating and detaining war criminals and enemy military personnel masquerading as civilians through contacts with the populace.

Section III. RELATIONSHIP WITH MILITARY POLICE

14–10. General

Counterintelligence and MP units have many parallel functions and responsibilities which, in some cases, may overlap; therefore, close coordination is essential for both units to be fully effective.

14–11. Specific

Counterintelligence and MP units have mutual interest in the following areas; primary responsibility may be vested in either unit.

a. Intelligence. Military Police develop police intelligence based on criminal and operational intelligence. Criminal intelligence pertains to individuals and organized crime activities while operational intelligence pertains to security and other MP activities. Both CI and MP units frequently will develop information of mutual interest which should be shared at the lowest practical level consistent with command policy on coordination.

b. Subversion. Military Police are concerned with the impact of organized crime on the war effort as well as the ties top criminals might have with local political leaders, political parties, labor unions, legitimate businesses, and governmental agencies.

c. Sabotage. Terrorism through sabotage is a criminal act as well as a coordinated enemy effort.

d. Refugee Screening. Military Police have control and evacuation responsibilities and can, with the assistance of furnished indicators, assist CI in spotting hostile intelligence, agents, saboteurs, subversives, and other dissident groups using the refugee and prisoner of war streams as a cover.

e. Rear Area Security. Both MP and CI elements can develop offensive and defensive measures in the ASCOM and TASCOM areas of the US Forces to deny the enemy information and materiel for hostile actions.

f. Harbor Security. Military Police elements can either organize or conduct patrols, security
surveys, or surveillance of suspected criminal groups in harbor areas.

**g. Circulation Control.** Military Police can devise registration and identification systems for the populace, set curfews, establish checkpoints, devise a pass system, and collect and analyze the modus operandi for criminal and hostile elements within the area of operation.

**h. Physical Security.** Military Police set up physical security measures including but not limited to the following: barriers, sentry dogs, alarm and anti-intrusion systems, guards, restricted areas, and perimeter lighting of key installations.

**i. Border Security.** Military Police are responsible for setting up anti-infiltration methods designed to keep the border secure from infiltration by enemy, neutral, and criminal elements.

**j. Civil Disturbances.** Military Police develop police intelligence and practice mob, riot, and crime control measures during civil disturbances.

**k. Others.** Many other areas exist, which would require coordination between MP and CI elements, such as espionage incident to the investigation of a crime, raids, or cordons and searches conducted jointly by MP and CI for various purposes; and mobile and static checkpoints manned jointly for either MP control purposes or CI spot checks for infiltrators.

### 14-12. Reciprocal Intelligence

The areas above indicate the extreme need for reciprocal intelligence and close coordination between MP and CI elements. For instance, the MP need intelligence on impending or actual refugee movements. This reciprocal intelligence can be obtained formally through staff elements or on a liaison type basis between operations officers or liaison personnel.

### Section IV. RELATIONSHIP WITH PSYCHOLOGICAL OPERATIONS

#### 14-13. General

Psychological operations elements have assigned interrogators who gain information from prisoners of war, detainees, or the local populace for attitude assessment and analysis, and target vulnerability analysis.

#### 14-14. Specific

Psychological operations are geared to assist the military effort in the following areas of CI interest.

**a. Consolidation Operations** are directed toward the populace of liberated or occupied areas to facilitate military operations and promote maximum cooperation.

**b. Populace and Resources Control** includes the announcement and reasons for restrictions placed on the populace as well as education for such programs as resettlement and clear and hold operations.

**c. Reeducation** is directed at prisoner of war and civilian detainees for the neutralization of their hostile attitudes and reorientation toward the US Forces.

**d. Area Estimates** are necessary for the conduct of PSYOP within an area of operations and will assist the CI data base.

**e. Media Analysis** is necessary for the discovery of clandestine subversive printing presses and other mass media, subversive activities within an area of operations.

**f. Black and Grey Propaganda** consist of covert PSYOP which do not disclose their source of origin. See FM 30-17A for CI aspects of these types of propaganda.

**g. Subversive Propaganda** is of interest to CA, PSYOP, and CI elements for the sake of planning countermeasures and can be a source of leads to CI elements.

**h. Others.** This includes objectives such as a nation building, cordon-and-search operational assistance, and the referral to CI of individuals who have potential for CI special operations.

### Section V. RELATIONSHIP TO OTHER INTELLIGENCE ELEMENTS

#### 14-15. General

**a.** Since CI units are charged with the overt liaison functions between local police, intelligence, and security organizations, other elements engaged in classified activities may also use the services of CI elements to perform necessary liaison activities.
b. Other MI elements can also assist CI elements in fulfilling their mission:

(1) Imagery Interpretation (II). II elements can interpret imagery designed to confirm a source's information or furnish imagery designed for briefings and debriefings of sources.

(2) Order of Battle (OB). OB personnel can keep the CI element updated on changing unit designations, compositions, and dispositions.

(3) Technical Intelligence (TI). TI personnel can keep the CI element advised on changes in equipment and equipment capabilities.

(4) Signal Intelligence (SIGINT). SIGINT assists the CI effort by deriving information from the intercept, direction finding, and analysis of enemy communications, including clandestine transmissions. Details on SIGINT support to CI operations are contained in FM 32–1 (to be published).
APPENDIX A

REFERENCES

A—1. Army Regulations (AR)

15–6 Procedure for Investigating Officers and Boards of Officers Conducting
Investigations.

27–45 Release of Information and Appearance of Witnesses.

50–2 Nuclear Weapon Accident and Incident Control (NAIC).


55–203 Movement of Nuclear Weapons, Nuclear Components, and Related Classi-
ified Non-nuclear Material.


135–380 Release of Classified Information to Army National Guard, United States
Army Reserve, and Reserve Officers’ Training Corps.

190–22 Search, Seizure, and Disposition of Property.


195–6 Department of the Army Polygraph Activities.

195–10 Military Police Criminal Investigative Activities.


310–50 Authorized Abbreviations and Brevity Codes.

340–2 Maintenance and Disposition of Records in TOE Units of the Active Army
and the Army Reserve.

340–15 Preparing Correspondence.

340–16 Safeguarding “For Official Use Only” information.

360–28 Guidance for Conduct of Information Actions in Support of Army Air
Defense Command Missile Program.

360–65 Establishment and Conduct of Field Press Censorship in Combat Areas.

360–81 Command Information Program Objectives and Policies, Publications, and
Armed Forces Radio and Television.


381-series Military Intelligence.

405–10 Acquisition of Real Property and Interests Therein.

600–3 Women’s Army Corps—General Provisions.

600–20 Army Command Policy and Procedure.

600–31 Flag Control Procedures for Military Personnel in National Security Cases
and Other Investigations of Proceedings.


606-series Personnel Identification.

611–15 Nuclear Duty Position Reliability Program (Reports Control Symbol
OPO-133).

(O)614–31 Assignment and Travel Restrictions.

(C)614–32 Restrictions of Assignment and Travel of Personnel Having Access to Spe-
cial Intelligence (U).
633-50 Prisoners of War; Administration, Employment and Compensation.
633-51 Civilian Internees Administration, Employment and Compensation.
640-20 U.S. Army Intelligence Badges and Credentials.
640-98 Filing of Adverse Suitability Information in Individual Records and Review of Intelligence Files Consulted Prior to Taking Personnel Action.
690-1 Civilian Applicant and Employee Security Program.
(0)700-65 Nuclear Weapons and Nuclear Weapons Materiel.
710-2 Materiel Management for Using Unit, Support Units, and Installations.
930-5 American National Red Cross Service Program and Army Utilization.

A—2. Army Subject Schedule (ASubjScd)
19-29 Collection and Preservation of Evidence.

A—3. Department of the Army Pamphlets (DA Pam)
27-1 Treaties Governing Land Warfare.
27-100-series Military Law Review.
27-161-1 International Law, Volume I.
108-1 Index of Army Motion Pictures and Related Audio-Visual Aids.
310-1 Index of Administrative Publications.
310-3 Index of Doctrinal, Training, and Organizational Publications.
380-1 Commander's Handbook on Security.

A—4. Field Manuals (FM)
3-10 Employment of Chemical and Biological Agents.
3-12 Operational Aspects of Radiological Defense.
5-20 Camouflage.
5-25 Explosives and Demolitions.
5-30 Engineer Intelligence.
(C)5-31 Boobytraps (U).
11-40 Signal Corps Pictorial Operations.
19-series Military Police.
20-32 Landmine Warfare.
21-6 Techniques of Military Instruction.
21-26 Map Reading.
21-30 Military Symbols.
21-31 Topographic Symbols.
21-40 Chemical, Biological, Radiological and Nuclear Defense.
21-50 Ranger Training and Ranger Operations.
24-18 Field Radio Techniques.
24-20 Field Wire and Field Cable Techniques.
30-series Military Intelligence.
31-16 Counterguerrilla Operations.
31-20 Special Forces Operational Techniques.
(C)31-20A Special Forces Operational Techniques (U).
31-21 Special Forces Operations—US Army Doctrine.
(S)31-21A Special Forces Operations—US Army Doctrine (U).
A—6. Other References

(C) SR 380–350–2 Captured Enemy Documents (U).
TB (PMG-series) Provost Marshal General.
TM 11–401 Elements of Signal Photography.
TM 30-series Military Intelligence.
TOE 30-series Military Intelligence.
APPENDIX B
INVESTIGATIVE REPORTS

Section I. GENERAL

B-1. Introduction
The basic format for Agent Reports, Reports of Investigation and Summaries of Information will be completed as described in the appropriate sections of this appendix and chapter 7. Figures are used to show graphically how each type of report is to be completed.

B-2. Application
The purpose, use and rules of preparation of these reports are general enough so that very little deviation therefrom would be necessary in the field unless unusual situations exist. Since all reports presented herein are standardized, a report prepared by a Special Agent in one part of the world will be understood by a Special Agent in another part of the world if all rules are followed.

Section II. THE AGENT REPORT (DA FORM 341)

B-3. Rules of Preparation

a. General. Each Special Agent will write his own reports. Supervisors may edit for clarity, but must not alter the basic meaning or intent. Overprinted Agent Report forms with spaces to be filled in with appropriate data may be used to expedite the reporting of routine records checks and, in completely favorable cases, the recording of results of interviews with listed and developed character references. Agent Reports are normally written in narrative style, third person, simple past tense, and active voice, except when quoting the source or indicating a state of mind or condition. The use of simple, direct, standard English facilitates comprehension and reduces the risk of misinterpretation. Slang expressions, colloquialisms, vulgarisms, and technical or trade terms should be avoided. Expressions which reflect approval or disapproval by the Special Agent of the occurrences, persons, or objects being described should not be used. Statements should be such that they may be verified through independent investigation by checking records or other credible sources of information. Agent Reports must indicate what the Special Agent determined, not what he did. The detailed techniques and procedures used to develop the information will not be described in the Agent Report; they will be made a matter of local record through operational reporting procedures prescribed by the unit commander (fig B-1).

b. Identity of Persons or Organizations.

(1) The surname of the person, or the name, abbreviation, or short title of the organization which is the subject of an investigation will be written in upper case letters throughout all reports. The word "SUBJECT" written in upper case letters may be used as a substitute for the name of person or organization in the body of the report. When personal pronouns are used which refer to SUBJECT (e.g., HE or SHE) the pronouns will be written in upper case letters. The names of persons and organizations not the subject of investigation will be written with normal capitalization. After first being fully identified, the person being interviewed may be referred to as "Source." The word "Source" in this usage is always a proper noun.

(2) Each investigative document will positively identify persons who are the subjects of investigations or who are of sufficient intelligence interest to be considered cosubjects as defined in AR 381-45 by including full name, aliases, maiden names, sex, date and place of birth, and social security account number, occupation, and address. All other persons mentioned in investigative documents will be identified by full name,
AGENT REPORT

1. NAME OF SUBJECT OR TITLE OF INCIDENT
DOAKES, John Q.
MSG, 458-58-5821
AKA: GREEN, Anthony G.
DPOB: 18 March 1923, Richmond, Virginia

2. DATE SUBMITTED
14 December 1971

3. CONTROL SYMBOL OR FILE NUMBER
458-58-5821

4. REPORT OF FINDINGS

(START ON THIS LINE) This line is started on the third line from the above black line. Indent five spaces from left margin to type phase designation. Keep left margin no more than one letter space from left margin. Leave right margin a minimum of 3/4". This leaves enough space to enter the word LEAD, if applicable. (LEAD)

When there is more than one paragraph in the report, double-space between paragraphs. Exhibits will be shown in the body of the report as (EXHIBIT__). The number is omitted by the Special Agent in the field, and a Roman numeral will be entered by the Control Office.

(HEARSAY INFORMATION) is normally contained in a separate paragraph of the report.

AGENT'S NOTES: Indent five spaces, and begin two spaces below the body of the report.

(SECOND AGENT REPORT ON SAME PAGE) When more than one Agent Report appears on the same page, five spaces will separate the reports.

When the report is too long to be contained on a single page, two line spaces must be left at the bottom of the page. The word (continued) will be typed in the lower right-hand corner of Block No. 4.

(2 Line Spaces)

(continued) if necessary

5. TYPED NAME AND ORGANIZATION OF SPECIAL AGENT
JOHN Q. AGENT, 115th MI Group

6. SIGNATURE OF SPECIAL AGENT
/s/ John Q. Agent.

Figure B-1, Agent Report Format.
occupation, and address. Elements of a proper name which cannot be determined from source or from telephone books, directories, and similar references will be indicated by: "fnu" (first name unknown) in lieu of the given name, "NMN" for No Middle Name, "IO" for Initial Only, and "LNU" (Last Name Unknown) in lieu of the surname. Names will be written in accordance with the custom of the country of which the person is native. (For example, some oriental names are written with the surname first.)

(3) Once a person has been identified fully, as indicated above, he or she will be referred to thereafter only by surname (without any titles such as Mr., Mrs., Dr., or Professor), unless there is more than one person with the same surname mentioned in the same Agent Report.

c. Numbers. Numbers from one to ten, inclusive, except in dates, addresses, or military unit designations, will be spelled out. All other numbers will be written in arabic numerals. In the case of money, numerals will be used regardless of the amount. Rather than writing $10.00, write $10.

d. Time. The military form will be used (e.g., 1605 hours).

e. Dates. The military form will be used (e.g., 26 January 1967). The names of months will be spelled out in full. Significant conflicts in dates will be resolved by investigation before cases are considered complete. Unexplained overlap in dates sometimes occurs when persons completing personal history statements and persons maintaining employment, education, and similar records, fail to show part-time employment, part-time attendance at educational institutions, breaks in employment, residences, etc.

f. Addresses. Addresses will be as complete as possible and written in the manner in which they are written in the United States. The names of cities, towns, counties, or other political subdivisions less than a state, will be written out in full. In foreign countries the use of UTM coordinates for cities, towns, or other locations is encouraged when necessary for positive identification. Repetitious or unnecessary use of coordinates should be avoided.

g. States and Countries. The name of a state will be spelled out when it first appears in a report. Subsequently, the state may be abbreviated if it is used as part of an address, except that a state name with five letters or less will not be abbreviated. The names of countries other than the United States of America (US) and the Union of Soviet Socialist Republics (USSR) will not be abbreviated.

h. Abbreviations. Abbreviations should be kept to a minimum. Standard military abbreviations, as outlined in AR 310–50, or standard civilian abbreviations as given by a "desk" or "collegiate" dictionary may be used in an address or as a means of identity; e.g., CPT for Captain (no period is used) or Dr. for doctor (a period is used). When brevity is appropriate, the title should be spelled out when used the first time in the report and the abbreviation or short title placed in parentheses directly after it; thereafter, throughout the report the abbreviation or short title may be used without parentheses; e.g., Johns Hopkins University (JHU), and later only JHU.

i. Standard Capitalization. The initial letters of proper nouns should be capitalized, such as James H. Brown, Captain, Infantry, 01925940, Commanding Officer; William F. Jones, Professor of English; Howard Snow, Vice-President, the University of Missouri; SUBJECT joined the Progressive Party; SUBJECT studied English, French, political science, history, and philosophy; HE moved to the West Coast; in the Summer of 1959, HE entered the US Army, but HE received a discharge in the Fall of 1959.

j. Units of Measure. Units of measure used in reports will be those given by the source. An approximation of conversion of the indicated measures stated in terms of the United States system of weights and measures will follow in parentheses. Whenever measurements must be made or estimated by the Special Agent, they will be stated in terms of the United States system of weights and measures.

k. Titles and Foreign Terms. In titles of publications, ships and plays, capitalize the first and all words except articles, prepositions and conjunctions. Foreign terms normally should be avoided; however, if used, they should have the English translation placed within parentheses following the first usage; e.g., Arbeitsamt (Labor Office). When printed, foreign words and phrases, titles of books, plays, magazine names, newspaper names, and names of ships are italicized, but when typewritten, they are underlined.

l. Reporting Interviews. Statements made by interviewees normally will be reported in substance.

m. Quotations. Quotations present exceptions to the foregoing items. Whenever a verbatim quota-
tion is placed in a report, it will be written exactly as it was stated by source except that SUBJECT's last name or a substitute which refers to SUBJECT will be in upper case letters. When taken from a document, the quotation will be copied exactly, including misspellings or grammatical errors which will be called to the reader's attention by the use of the Latin word "sic," meaning "thus," immediately after the error.

n. Hearsay Statements and Opinions. Statements of this nature should be used primarily as the basis for further investigation, and if relevant and material to the issue, should be confirmed or disproved if possible.

o. Physical Descriptions. When it is necessary to physically describe individuals mentioned in Agent Reports, a complete physical picture of the individual should be presented (FM 19–20). Because the information and characteristics for identifying persons lends itself well to tabulation, the following format may be used:

Name:
Age:
Sex:
Race:
Height:
Weight:
Build:

Other specific information or physical characteristics may be woven into this sequence or added to the sequence when data is available. In addition if an Identikit was used, the montage codes can be tabulated to permit any other agency to reassemble the composite likeness of the subject. All the montages used in the composite must be listed. Offices not having an Identikit may be able, through liaison, to have another investigative or intelligence agency to reassemble the composite.

p. Tabulated Material. Although Agent Reports normally are written in narrative style, there are times when material can best be presented in tabulated form. Descriptions, certain records checks, and lists of persons and addresses, for example, may be tabulated to the advantage of both writer and reader. All 201-file checks and birth records checks should be reported in tabulated form. Tabulated material will be presented in the following manner: One line space will be provided between the body of the report and the tabulation, but none between the items being tabulated. Use open punctuation; i.e., no end punctuation should be used in any tabulations. The left-hand column of items should be indented five spaces from the left margin. If any tabulated item in this column requires more than one line, the additional line or lines are indented three additional letter spaces within the column. The right-hand column of items should be typed two spaces to the right of the longest item in the left-hand column. Any item in this column which requires more than one line will be typed without additional indentation. Subparagraph numbers or letters are not used with the items being tabulated (fig B-2).

B–4. Format

DA Form 341, the Agent Report form, has been designed to facilitate recording the results of investigative activity in a uniform, well-organized complete fashion.

a. Block No. 1, Title Block. The title block for an Agent Report is always the same as the title block of the pertinent request for investigation except that any aliases or other essential data developed as a result of the investigation also will be inserted. All cases which are closely related should bear cross-references. Such cross-references are entered in Agent Reports as prescribed by local procedures. Leads or other information reported in an Agent Report do not affect the title block. If a Special Agent originates an Agent Report in cases where there is no pertinent Lead Sheet or other request for investigation, an appropriate subject or title will be inserted. The subject block of the Agent Report will be prepared as follows:

(1) Persons. Subject blocks will contain in columnar arrangement: SUBJECT's name, rank and social security number (SSN), any other names (i.e., aliases, pen names, etc.), and date and place of birth (all on one line) as in the following examples:

(a) BURNS, John E.
   LTC, 561–54–6706
   AKA: Green, Anthony T.
   DPOB: 25 December 1925, Athens, Ohio
(b) JONES, Mary Ann
   NEE: Williams
   SSN: 212–40–2306
   DPOB: 10 September 1945, Reno, Nevada

Open punctuation is used in the subject block.

(2) Organizations. In the investigation of or-
<table>
<thead>
<tr>
<th>1. NAME OF SUBJECT OR TITLE OF INCIDENT</th>
<th>2. DATE SUBMITTED</th>
<th>3. CONTROL SYMBOL OR FILE NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSG, 458-58-5821</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AKA: GREEN, Anthony G.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DPOB: 18 March 1923, Richmond, Virginia</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4. REPORT OF FINDINGS

(Listed Character Reference)*

(Developed Character Reference)*

a. DATE INTERVIEW CONDUCTED:

b. INTERVIEWEE:

c. OCCUPATION:

d. RESIDENCE:

e. Social Security Account Number:

f. Subject's Name with Aliases:

g. Length of Acquaintance:

h. Type of Contact:

i. Degree of Association:

j. Last Seen:

k. Names of Parents & Siblings:

l. Marital Status:

m. Residences:

n. Education:

o. Employment:

p. Character & Reputation:

q. Honesty and Integrity:

r. Personal & Financial Habits:

s. Mental Stability and Maturity:

t. Political Proclivities:

(continued)

5. TYPED NAME AND ORGANIZATION OF SPECIAL AGENT:

JOHN Q. AGENT, 115th MI Group

6. SIGNATURE OF SPECIAL AGENT:

/s/ John Q. Agent

Figure B-2. Columnized Agent Report.
AGENT REPORT: (LCR) RE: Subject's name; DPOB; Date of Report, (Names of Interviewee(s))

4. REPORT OF FINDINGS:
   u. Organizations : 
   v. Foreign Travel : 
   w. Relatives in Foreign Countries : 
   x. Loyalty : 
   y. Recommendation for Position of Trust : 
   z. Throw Offs : 
   aa. Remarks : 

*Type in or overprint the appropriate phase designation. Use only when results are favorable.

Signature of Special Agent________________________ page 2 of 2

Figure B-2. Continued.

organizations, the subject block will contain the name and, if applicable, the address of the organization. The name will be written entirely in upper case letters and may be followed by an abbreviation or short title to be used in the report as a substitute for the organization's name. Care should be taken to insure that the abbreviation or short title chosen is not ambiguous or misleading. When a foreign organization is the subject of an investigation, or when it appears as a possible lead, it is recommended that the following items of identity be included at least once in the body of the report:

(a) Full title in English alphabet characters and in native writing (for non-Latin names only).

(b) English translation (for all foreign languages) and short title, when appropriate.

(c) Former name or names (when definitely known).
(d) Address (headquarters, branch, or office, as applicable).

(e) Nationality, when needed for better understanding.

(3) Incident. The investigation of an incident is a specialized type of investigation. The incident case title should answer three questions in the following order: what, where, and when. In incident cases, normal capitalization will be used for each word except that prepositions, articles, and conjunctions, when not the first word of a title, will not be capitalized. Although incident cases eventually may involve known persons, or perpetrators may be revealed, the initial title of an incident case should not be changed. This does not preclude opening a separate case with a new individual title on a person mentioned in an incident case if the new case concerns activity not a part of the incident case.

b. Block No. 2, Date Submitted. The date the report is prepared by the Special Agent is entered in normal military style without abbreviations.

c. Block No. 3, Control Symbol or File Number. This space will contain the file or dossier number of the investigation as prescribed by AR 381-45 and assigned by the Control Office.

d. Block No. 4, Report of Findings.

(1) Format. The report will start on the third line space from the black line at the top of block No. 4, thus leaving two blank lines at the top of block No. 4. Also, when the report is too long to be contained on a single page, two blank lines must be left at the bottom of the page, and additional DA Forms 341 may be used or plain bond paper 8 x 10 1/2 can be used as illustrated in figure B-2. A margin of no more than one letter space from the vertical black line on the left side of the page and a minimum 3/4-inch margin from the black line on the right side of the page will be maintained at all times. The first line of a paragraph should be indented five spaces from the left margin; a double space is left between paragraphs. Proper paragraphing and spacing are illustrated in sample reports included as figures to this appendix. The blocks Nos. 1, 2, 3, 5, and 6 will be completed in full on all pages if DA Form 341 is used. If bond paper is used, the example as shown in figure B-2 is mandatory. A system for numbering of pages may be prescribed in the unit SOP. Unless otherwise instructed, Special Agent will not number Agent Reports or the paragraphs of the report; however, paragraphs of classified reports will be marked in accordance with AR 380-5. Numbering of reports normally will be done by the office preparing the Report of Investigation (fig B-3).

(2) Phase designation. In background investigations, the first item in the first paragraph of the Agent Report will be the designation of the phase of the investigation most applicable to that report. Normally, the Agent Report is the written result of a single investigative activity; that is, one report will be devoted to each source of information. Occasionally, reports concerning sources that satisfy the same investigative phase may be included on the same form. For example, a verification of education by records check and an interview with a former teacher or classmate—both activities conducted by the same agent at the same school—may be included on the same form since both concerned the education phase. Where more than one such report appears on a page, five spaces will separate the reports, and each will begin with the phase designation. There is an exception to the requirement that one Agent Report will be a record of a single investigative activity; when interviews of several persons (again satisfying the same investigative phase) concerning the same individual or the same incident produce substantially the same favorable information, these interviews may be combined into one Agent Report. Each interviewee must be completely identified, and the duration and extent of his knowledge of SUBJECT or of the incident must be stated. However, when adverse, derogatory, or conflicting information is obtained, each report will be recorded on a separate report form. The first paragraph of each report will begin with the phase designation in upper case letters enclosed in parentheses. Generally, the phase designation covers that part of SUBJECT'S life of which the source has most knowledge. Following are some of the standard phase designation headings:

(NATIONAL AGENCY)
(NATIONAL AGENCIES)
(LOCAL AGENCY)
(LOCAL AGENCIES)
(MILITARY SERVICE)
(MEDICAL RECORDS)
(201-FILE CHECK)
(CIVILIAN PERSONNEL RECORDS)
(CITIZENSHIP)
(BIRTH)
(LISTED CREDIT REFERENCE)
(DEVELOPED CREDIT REFERENCE)
(LISTED CHARACTER REFERENCE)
(DEVELOPED CHARACTER REFERENCE)
AGENT REPORT
(AR 381-130; FM 30-17)

1. NAME OF SUBJECT OR TITLE OF INCIDENT
GREER, John A. II
DAC, Adm Asst, GS-12; Gl, SSAN: 063-36-2179
DPOB: 7 May 1924, Bayside, New York

2. DATE SUBMITTED
15 January 1971

3. CONTROL SYMBOL OR FILE NUMBER
063-36-2179

4. REPORT OF FINDINGS

(EDUCATION) On 14 January 1964, the following persons were interviewed, separately, concerning John A. GREER II, at the College of Business, Middle State University, 2460 Hyde Park Boulevard, Chicago, Illinois, and they furnished substantially the same information:

- James J. Collins, Assistant Professor, 319 Edward Street, Chicago, who knew SUBJECT from 1946 to 1950 as a classmate.
- Henry C. Adams, Administrator, 217 Oakdale Avenue, Chicago, who knew SUBJECT as a classmate from 1946 to 1950.
- John R. Williford, Personnel Director, 1 Wilson Avenue, Chicago, who knew SUBJECT as a student from 1946 to 1950.

Sources had no social contact with SUBJECT and were only associated with HIM in an educational capacity. They have neither seen nor corresponded with GREER since the Summer of 1951 when they met at a class reunion on the university campus.

SUBJECT was an exceptional student and received an award in HIS senior year for writing an article on "cost-plus" construction. HE was well liked by students and faculty. HE belonged to no organization. While at college, HE held a part-time job with a construction firm in Chicago. Additional information concerning HIS employment is not known.

SUBJECT's closest associate while at school was Harry L. Waldrop, 4433 West Alameda Parkway, Des Moines, Iowa, who was an accounting major with whom HE did much of HIS research at the university. HE was also closely associated with Barbara M. Koncher, 320 South Beach Street, Atlanta, Georgia, a member of the Chi Alpha sorority, whom HE dated frequently.

Sources had no reason to question GREER'S moral character, honesty or trustworthiness. SUBJECT never made any statement or performed any act, in Sources' presence, that would be considered inimical to the best interests of the United States. HE indulged in the moderate use of alcoholic beverages. Sources had no knowledge of SUBJECT'S financial reliability; however, they have never heard anything unfavorable concerning HIS financial status. To the best of Sources' knowledge, SUBJECT has never traveled outside the United States and HE has no relatives or financial interests in any foreign country.

(continued)

5. TYPED NAME AND ORGANIZATION OF SPECIAL AGENT
JOSEPH S. ANDERS, 113th MI Group

6. SIGNATURE OF SPECIAL AGENT
/s/ Joseph S. Anders

Figure B-3. Example of a completed Agent Report.

Sources recommended that John A. GREER II be considered for assignment to a position of trust and responsibility with the US Army.

Signature of Special Agent

Page 2 of 2

Figure B-8.—Continued.
The Special Agent will occasionally have need for phase titles to fit particular situations such as (NEIGHBORHOOD CHECK), (SURVEILLANCE), or (SUBJECT INTERVIEW). To facilitate review the agent may have need of multiple phase titles, such as (BIRTH—EDUCATION), (EMPLOYMENT—DEVELOPMENT CHARACTER REFERENCE), or (EMPLOYMENT Coworker).

3. The body of the Agent Report. Here is recorded the information obtained by investigative effort. The Special Agent must organize the facts and present the information in a clear and logical manner, insuring that the information is accurate, complete, pertinent, clearly phrased, unbiased, and concise.

(a) Introductory element. The first sentence or paragraph of each Agent Report is known as the introductory element. The introductory element must contain, as appropriate, the complete identities of the individuals interviewed, the custodians of files checked, the records themselves, official and home addresses, and accurate locations of files checked. A secondary purpose of the introductory element is to permit the retracing of any previous investigative effort at a later date should it be necessary. An introductory element will include specific items of information arranged in the following manner:

1. Interviews (background investigations). The phase designation; date of interview; identity of interviewee (to include full name, occupation, complete address, SSN, and, in the case of military personnel, full name, grade, branch of service for officers, SSN, position or job title, and complete official address); and place of interview if other than address listed. The period of knowledge, and the relationship of the interviewee to SUBJECT will be stated briefly.

2. Interviews (incident investigations). Date of interview; complete identity of source; place of interview; and, if applicable, the reason for interview.

3. Surveillance. The date, duration, type, name of subject of surveillance (if other than SUBJECT, and all possible identifying data concerning the person or persons under surveillance); place; and identity of person or persons conducting the surveillance. If the situation necessitates protection of the identity of the person or persons other than Special Agents conducting the surveillance, a coded reference will be prescribed.

4. Record checks. Phase designation (in background investigations); date of check; location of record; office or other location; name and position of the person who sought the record or made it available (Special Agent must indicate whether he personally examined the record or if the information was orally furnished to him); full identity of the record; i.e., volume, title, page, date, or similar appropriate information when available (fig B-4).

5. Raids, searches and seizures. The date of the activity; identity of persons and/or units conducting such activity; and authority for such activity. In searches or seizures, the name of the witnessing officer (usually the individual's commanding officer or his designated representative) will be included.

6. Attempt. Phase designation; date of attempt; identity of intended interviewee or record (as above); identity of person(s) spoken to; reason why intended interviewee or record was not available; and any possible leads. The explanation should clearly indicate that all possibilities to locate the intended source of information were exhausted (fig B-5, B-6).

7. Confidential source. Confidential sources who have been coded for security purposes will not be identified nor will information or phraseology tending to identify, pinpoint, or compromise them appear in investigative reports. Confidential sources will be referred to only by their designated code or symbol, e.g., source R-S-17. The source of the information will be mentioned only once in the Agent Report and that will be in the introductory element. To assist in the evaluation and adjudication processes, the Special Agent will indicate by word picture the degree of reliability of the source when submitting information derived from them. Where the word picture proves inadequate in determining reliability, additional clarifying comments may be made in the introductory element or in Agent's Notes. The word picture, which may be used only for coded confidential sources, may be as outlined below though not necessarily confined to these examples:

(a) Source, who has furnished reliable information in the past . . .

(b) Source, who has furnished information corroborated in part or in whole by other sources . . .

(c) Source, whose reliability is unknown, but who has been an acquaintance of SUBJECT for the past 5 years . . .

(b) Information obtained. Following the introductory element, a new paragraph will contain the information obtained by the investigative
**AGENT REPORT**

1. NAME OF SUBJECT OR TITLE OF INCIDENT

   DOAKES, John A.
   MSG, 458-58-5821
   DPOB: 18 March 1923, Richmond, Virginia

2. DATE SUBMITTED

   15 December 1970

3. CONTROL SYMBOL OR FILE NUMBER

   458-58-5821

4. REPORT OF FINDINGS

   (LOCAL AGENCY) On 15 December 1963, records checks concerning John A. DOAKES were conducted at the following listed agencies with the results as indicated:

   - Police Department, Baltimore, Maryland No Record
   - Baltimore Office, FBI, Baltimore, Maryland No Record
   - Provost Marshal's Office, Ft. Holabird, Md. No Record

5. TYPED NAME AND ORGANIZATION OF SPECIAL AGENT

   JOHN Q. AGENT, 109th MI Group

6. SIGNATURE OF SPECIAL AGENT

   /s/ John Q. Agent

---

*Figure B-4. Example of a LAC-Type agent report.*
**AGENT REPORT**

(AR 381-130; FM 30-17)

1. NAME OF SUBJECT OR TITLE OF INCIDENT
   DOAKES, John A.
   MSG, 458-58-5821
   DPOB: 18 March 1923, Richmond, Virginia

2. DATE SUBMITTED
   14 December 1970

3. CONTROL SYMBOL OR FILE NUMBER
   458-58-5821

4. REPORT OF FINDINGS

   (LISTED CHARACTER REFERENCE) On 14 December 1970, an attempt was made to interview Mr. Leslie J. Warren, 2317 St. Paul Court, Seattle, Washington, concerning John A. DOAKES. Mrs. Ray Smallwood, owner of the building, 2317 St. Paul Court, Seattle, stated that Warren had moved from that address in February 1969. His forwarding address is 516 Flagstone Avenue, El Paso, Texas. (LEAD)

5. TYPED NAME AND ORGANIZATION OF SPECIAL AGENT
   JOHN Q. AGENT, 115th MI Group

6. SIGNATURE OF SPECIAL AGENT
   /s/ John Q. Agent

---

_Figure B-5. Example of an attempt-type agent report (Lead)._
1. NAME OF SUBJECT OR TITLE OF INCIDENT
DOAKES, John A.
MSG, 458-58-5821
DPOB: 18 March 1923, Richmond, Virginia

2. DATE SUBMITTED
14 December 1970

3. CONTROL SYMBOL OR FILE NUMBER
458-58-5821

4. REPORT OF FINDINGS
(NEIGHBORHOOD CHECK) On 10 April 1962, a neighborhood check was conducted in
the vicinity of 3709 Grand Avenue, Oasis, California, in an attempt to locate per-
sons with a knowledge of SUBJECT. Joe Jenkins, landlord of 3709 Grand Avenue,
statement that he purchased the property in 1958 and did not have a list of the
rents who lived in this property at the time of SUBJECT'S residence. Jenkins
did not know SUBJECT and could not suggest anyone with knowledge of HIM.

S A M P L E

5. TYPED NAME AND ORGANIZATION OF SPECIAL AGENT
JOHN Q. AGENT, 115th MI Group

6. SIGNATURE OF SPECIAL AGENT
/s/ John Q. Agent

Figure B-6. Example of an attempt-type agent report (No-Lead).
efforts of the Special Agent. In the case of personnel security investigation (SPI) interviews, a definite and logical pattern should be followed.

1. Relationship paragraph. The report of interview should begin with a complete and thorough treatment of the relationship between the interviewee and the subject. This information may be contained in a separate paragraph referred to as the “relationship paragraph.” More specifically, under what circumstances, to what extent, and exactly when the interviewee knew the subject. A simple but effective way to begin a relationship paragraph would be, “Source first met ABLE in April 1958 . . .” Then complete the relationship paragraph concisely with appropriate factual statements pertaining only to the nature, degree, and duration of the association between Source and ABLE, and conclude with a concise statement as to when Source last saw ABLE or communicated with HIM. The purpose of a good relationship paragraph is to permit the reader to form an opinion as to the general reliability of the information which should follow.

2. Background information. In most PSI interviews, background information pertinent to the subject is obtained. This may be placed in a paragraph immediately following the relationship paragraph. Background information should be reported chronologically. This background data may verify or give basis to doubt information reported by the subject on his statement of personal history. A discrepancy between statements of source and SUBJECT will require additional investigative effort. Confinement of this type of information to a separate paragraph permits the Special Agent to devote the remainder of the report to a full treatment of the information regarding loyalty, integrity, discretion, morals, and character with which the BI is primarily concerned. More than one paragraph pertaining to background information may be needed in certain cases.

3. Narrative report of interview. Complete reporting is achieved only by a thorough expository treatment of the subject’s loyalty, integrity, discretion, morals, and character, in addition to a routine chronology of personal history. The element of loyalty will be stressed in all background investigations and, where applicable, in complaint investigations. Subject’s financial responsibility, emotional stability, and social habits should also be determined. Questions concerning religious, racial, or political matters should not be raised unless absolutely necessary and pertinent to the purpose of the investigation. When derogatory information is furnished in the course of an interview, pertinent and relevant statements made by interviewees should be quoted verbatim, or as near verbatim as possible. In all such cases, after obtaining all available information, the Special Agent should ask the interviewee whether he is willing to—

(a) Submit a sworn statement.
(b) Have his information made known to the subject.
(c) Be identified to the subject as the source of the information.
(d) Appear before a proceeding in open or closed session.

Interviewee’s answers to the above questions will be included in the narrative report of interview. A sworn statement will be obtained if possible and attached as an exhibit to the Agent Report. In those cases where the answers to any of the above questions are negative, an attempt should be made to determine and record the reason for refusal. When the source who has given derogatory information about the subject requests anonymity, the investigative effort must be extended to further develop such information and to safeguard the identity of the source. A key sheet, DA Form 2357-R (fig B-7) which will be locally reproduced on 8-x 10 1/2-inch paper, will be prepared and forwarded as a separate element of the investigative file; access to it will be limited to adjudicating authorities and review boards or panels. The source will be referred to by code in the Agent Report. Should the interviewee provide hearsay information or rumors, the original source of which cannot be determined or to which confirming or refuting leads cannot be developed, a separate paragraph, clearly labeled as hearsay, will be included in the Agent Report. The paragraph will be started with the words (HEARSAY INFORMATION) in upper case letters and inclosed in parentheses.

4. Recommendation paragraph. The last paragraph of background investigation interview reports will contain the interviewee’s recommendation concerning the advisability of appointing the subject to a position of trust and responsibility with the US Army. The Special Agent should make every effort to obtain a definite positive or negative recommendation from the interviewee and avoid qualifying remarks. If interviewee declines to give any recommendation, his reasons will be a part of the last paragraph as will any restriction he places on the use of his information and his willingness to testify at board hearings. In certain cases when the subject has demon-
<table>
<thead>
<tr>
<th>1. SUBJECT</th>
<th>2. DOSSIER NUMBER</th>
<th>3. DATE FORWARDED</th>
<th>4. KEY SYMBOL IDENTITY CODE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5. NAME OF SOURCE</th>
<th>6. POSITION OF SOURCE IN RELATIONSHIP TO SUBJECT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7. EVALUATION OF SOURCE AND INFORMATION GIVEN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8. REASON FOR CODING (Check one and add further explanation if necessary)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Divulging the identity of Source will have an adverse effect on national security (Confidential Source).</td>
</tr>
<tr>
<td>The Source refuses to be confronted and wishes to remain anonymous. Include reason, if given.</td>
</tr>
</tbody>
</table>

THIS SHEET IS NOT PART OF THE INVESTIGATIVE FILE.

DA FORM 2357-R, 1 SEP 60

Figure B-7. DA Form 2357-R, key sheet.

strated his unreliability (e.g., AWOL and defectors) a recommendation is not required from interviewees. Instead, a statement will be included to the effect that source will notify proper military authorities should additional pertinent information arise.

(4) Agent's notes. Agent's notes are an addendum to the Agent Report and are placed after the concluding paragraph of the report. Agent's notes are used to aid the reviewing officers in their study and evaluation of the information reported and to draw attention to pertinent discrepancies. Agent's notes should contain only comments and opinions of the Special Agent; all information obtained by investigation must be stated in the body of the report. The reasons for
the Special Agent's opinions should be evident; if not, the reasons must be made clear. Comments will be presented as concisely as possible.

(a) Agent's notes may be used to—
1. Call attention to, and set forth reasons why, the Special Agent did not, or why others should not, follow up an obvious lead if not otherwise apparent.
2. Give facts from the Special Agent's knowledge of the area or situation, otherwise not apparent, which might help to clarify an issue.
3. Give pertinent information concerning the source, which for any reason is not included in the body of the report, e.g., adverse comments concerning the reputation, competency, or credibility of the source, or competency in the language in which the interview was conducted, if relevant.
4. Give the Special Agent's opinion of the interviewee (bias, prejudice, senility, etc.) or of the information obtained, if necessary for clarification or proper evaluation. This should be stated as an opinion, never as a fact.
5. Point out discrepancies in subject's statement of personal history, conflicting information submitted in other reports, and cross-reference to related material.
6. Point out the condition of records, if this might affect their validity or reliability.
7. Explain any unusual terms or words in the paragraph if such explanation requires more than one word placed in parentheses after the term.
8. Draw attention to conflicts or discrepancies in different accounts of the same matter and state the Special Agent's opinion, supported by his reasons, as to which is the more reliable version.
9. Indicate whether two sources having the same last name are related.
10. Make reference to other related reports in the same case.

(b) Agent's notes will not be used to—
1. Provide a catchall for nonpertinent information.
2. Call attention to minor discrepancies in dates of employment or education and in house numbers of listed street addresses. It is preferable in such cases to focus attention by underlining the information at variance.
3. Take the place of a negative report. When effort by the Special Agent fails to locate an interviewee or a record, this effort will be recorded in a separate Agent Report as an attempt.
4. Describe the difficulties experienced by the Special Agent in contacting the source, unless this reflects on the source's reliability.
5. Refer to internal correspondence or forms peculiar to the local unit.
6. Indicate recommendations.

(c) When used, agent's notes will be placed at the conclusion of the Agent Report to which they pertain. The designation will be typed in upper case letters, i.e., “AGENT’S NOTES,” followed by a colon. Agent's notes are indented five spaces and are contained in one paragraph regardless of the diversity of the contents. Agent's notes will begin two spaces below the last line of the Agent Report to which they pertain.

e. Block No. 5, Typed Name and Organization of Special Agent. The reporting Special Agent's name will be typed in upper case letters in normal order followed by the intelligence unit designation.

f. Block No. 6, Signature of Special Agent. The investigating Special Agent's signature will appear as typed in block No. 5. The agent will personally sign in ink all copies of the Agent Report when it contains adverse or derogatory information or concerns a complaint type investigation. Variations of this policy may be authorized by the investigating unit in individual cases for unusual circumstances. Agent Reports not concerned with complaint type investigations and containing no derogatory or adverse information may be signed for the investigating Special Agent by an individual responsible for the authenticity of the reports.

B-5. Leads

a. A lead is any information collected during an investigation which may require further development of investigation. It may be the name, address, or location of a person, firm, or organization. It is usually a source which can furnish further information on the case or which can lead to additional information. Leads are included in the Agent Report paragraph as information obtained.

b. Initially, the Control Office extracts leads from subject's statement of personal history. Normally, these initial leads are distributed by means of DA Form 339 (Lead Sheet) (AR 381-130) to the MI units that will conduct the investigation. The leads noted on Lead Sheets or contained in Agent Reports must be specific and complete, so that the investigative activities may be conducted intelligently and thoroughly.

c. Leads collected during an investigation, e.g.,
“throwoffs” or other developed references not contained in a Lead Sheet, are subsidiary leads. Normally, the reporting unit is authorized to develop all subsidiary leads within its own area of jurisdiction. Therefore, if the lead can be developed by the reporting agent or by someone within the jurisdiction of the command, no formal indication of the lead is necessary. This type lead is referred to as a “jurisdictional lead.” However, when the lead is outside the jurisdiction of the reporting command, necessitating communication with an MI group in another command, the Special Agent will formally indicate the lead in the Agent Report in the following manner: The word “(LEAD)”, typed in upper case letters and enclosed in parentheses, will be placed in the 3/4-inch marginal space on the right of the Agent Report on the line in which the lead is first mentioned. The closing parentheses will be flush to the back vertical line on the form. This type of lead is referred to as an “indicated lead.” Leads naming persons, firms, or organizations known to the reporting Special Agent as being suspect or subversive are also indicated. The reason for indicating such leads will be reported in Agent’s Notes.

B–6. Exhibits

To amplify or to confirm information contained in Agent Reports, particularly if they prove or disprove derogatory information, or provide evidence of the nature of incidents and the manner in which they were caused, the Special Agent must submit available documentary and physical evidence. This evidence must be in the form of records, identification documents, affidavits, statements, photographs, transcripts of interviews, photostats, sketches (made by either the Special Agent or other persons), documents, pamphlets, newspaper clippings, and sound recordings. Exhibits or objects of physical evidence which are to be presented in legal proceedings must be maintained in a continuing chain of custody. Copies will be attached to the Agent Report as EXHIBITS. In the body of the report, the designation should follow immediately after references to the item attached. Example: “SCHMIDT wrote a letter (EXHIBIT I) to Charles B. Walker, Beverage Salesman, Tasty Beverage Company, 666 Dundalk Avenue, Baltimore, Maryland 21219.” Or: “Attached hereto is EXHIBIT I, (three pages) sworn statement, prepared by Jones dated 9 January 1960.” Normally in a PSI, the exhibit is not numbered by the Special Agent; the numbers (Roman numerals) will be inserted by the Control Office when the assembled Agent Reports and exhibits are organized for review and forwarding to the action agency. Exhibits must supplement, not replace, Agent Reports.

a. In preparing paragraphs concerning exhibits, the following procedures apply:

(1) When the source of information is a written record, it must be identified by office, location, title, volume, page number, and date. A copy of a portion of a record included as a part of an Agent Report will be designated as an “extract.” Care will be exercised in making extracts to insure that divorcing the passage from its context does not alter its meaning. A complete copy of a record will be designated as an “exhibit” and attached to rather than incorporated into the Agent Report. If the source of information obtained from written records is classified, or if the revelation of such source would compromise counterintelligence operations or embarrass the agency furnishing such records, the material in the reports may be paraphrased and the source referred to by code designation. The exact reference to the source will be maintained in a manner consistent with the security considered necessary by the responsible counterintelligence unit or appropriate Control Office. This information should be accessible, however, if required by further developments in the case.

(2) When the exhibit is a copy of an affidavit, a letter, or other document, the Special Agent must include all information which reveals how, where, when, from whom, and under what circumstances the exhibit was obtained. The substance of information contained in the exhibit will be included in the body of the Agent Report. The Special Agent must not omit any detail which indicates the value the exhibit has in relation to the purpose of the investigation. Facts which later may have a bearing on its probative or adjudicative value must be reported fully.

(3) The Special Agent will state in his report, or on the copies of the exhibits, the exact location, name, and title of the custodian of the original evidence. In some instances, the originals are not obtainable and copies must suffice, but the location of the original must be given in the report. In such a situation, the names and addresses of two persons who could testify to the authenticity and existence of the original should also be stated in the Agent Report. In the case of documents or copies of documents which are obtained covertly, the Agent Report transmitting them to higher headquarters must contain sufficient iden-
fying information to enable case officers to properly appraise their validity and importance.

(4) In the case of physical evidence, if the nomenclature of the material will not serve as a description, the Special Agent should describe generally the equipment or the apparatus so that the reader will be able to comprehend the physical characteristics and utilization of the material to which reference is made.

b. In preparing exhibits to be attached at the end of an Agent Report, the following procedures apply:

(1) The identifying data for each exhibit will be typed on the cover sheet. Cover sheets will contain the exhibit number, subject, file number(s), designation of the preparing unit, date of the Agent Report to which the exhibit(s) applies, and, when applicable, security classification.

(2) If an original documentary exhibit requires a security classification, the classification may be stamped on a backing sheet, a cellophane or other envelope, a permanent folder, or other means used which will keep the security classification or near the exhibit without defacing it. Duplicates of documentary exhibits are marked with the proper security classification in accordance with the provisions of AR 380-5. Newspapers and other public periodicals will not be classified, but the file may be classified to prevent disclosure of MI interest in this area.

(3) Original copies of documentary exhibits, which have been received from other sources, will not be marked in any way.

(4) Documentary exhibits normally will be prepared or mounted on 8- x 10 1/2-inch paper. Exhibits larger than 8- x 10 1/2 inches will be folded to such size, if this can be done without affecting their value. Where the exhibit is an identity document, pass, sample of stationery or item of possible counterintelligence operational use, the exhibit should be placed unfolded in a clean envelope after data identifying the exhibit has been placed on the envelope.

(5) Sworn statements are obtained in accordance with chapter 3.

(6) In all cases when serious derogatory documentary information is developed on a subject or when favorable documentary data is obtained which wholly or partially refutes adverse information, certified true, photostatic, or other authentic copies or extracts will be obtained to accompany and substantiate the report information. When it is impossible to accomplish the foregoing, the Special Agent should personally verify the information in the documents and so state in the Agent Report. If the documents are not made available for verification, a signed sworn statement by the document custodian will be obtained, if possible, concerning the contents. Lacking this, the Special Agent will obtain full identifying data concerning the custodian.

(7) Extreme care will be exercised in citing any local intelligence studies or reports which have not received Department of the Army evaluation. Reports or studies which have not been so evaluated normally will be referred to in Agent Reports only as an aid to supervisory and investigative control personnel in directing further investigation. Agent Reports containing such unevaluated reports or studies will not be included with the Report of Investigation prepared upon conclusion of an investigation. Properly evaluated data from local intelligence studies or reports may be entered in Agent Reports included with the Report of Investigation, provided the original source can be identified and his reliability established.

B-7. Information Obtained from Government Agencies

Charges or allegations of counterintelligence significance against personnel subject to Department of the Army jurisdiction are often received in the course of interviews or records checks from other government agencies. These charges or allegations, together with the evaluation of the source as given by the contributing agency, should be included in the Agent Report. When the agency reporting these charges is another investigative agency, no new investigation will be instituted without the approval of the reporting agency. This coordination will preclude the possibility of compromise to any investigation currently in progress.

Section III. REPORT OF INVESTIGATION (DA FORM 342)

B-8. Format and Preparation
The Report of Investigation is prepared according to the following procedures:

a. The accumulated Agent Reports are arranged in a logical order and each report is numbered in a single series with Arabic numerals.
This numeral is placed in the five-space indentation of the introductory element of each attached Agent Report. The logical order of the Agent Reports will vary as follows (fig B-8):

(1) In background investigations, the sequence of phase designations stated in AR 381-130 should be used.

(2) In complaint type investigations and incident investigations the scope and nature are so varied that no sequence can be prescribed. The sequence should logically present the development of the investigation.

b. The exhibits prepared for the investigation are arranged in numerical order using Roman numerals. Exhibits are numbered in the order in which they are mentioned in the numerically arranged Agent Reports and are placed as a group following the Agent Reports. Exhibits are never interspersed among the Agent Reports. Originals of exhibits will be retained by the control office with the open case file until required by the action agency or higher authority. However, originals will be included, if possible, in the closed case file which is forwarded to the US Army Investigative Records Repository (IRR), Fort Holabird, Maryland 21219. In instances when results of polygraph examinations are used as exhibits, instructions contained in AR 195-6 will apply.

c. DA Form 342 is prepared as follows:

(1) “Identifying Data” is the first major division of DA Form 342, and is composed of blocks 1 to 15. Definite entries are made in blocks 1 through 10 when the subject of an investigation is a known person or organization. The letters “NA” (not applicable) are entered in blocks 11 through 15 in this case. When the investigation deals with an incident in which the person or persons concerned are not known, blocks 11 through 15 will contain definite entries identifying the incident, and the letters “NA” entered in blocks 1 through 10.

(2) “Control Data,” the second major division of DA Form 342, is composed of blocks 16 through 18.

(3) “Investigative Data,” the last major division of DA Form 342 is composed of blocks 19 through 25.

(a) Block 22 indicates the status of the investigation. The status indicated must be one of the following:

1. Closed. An investigation is indicated as closed when no further investigative activity is necessary to enable proper authorities to make a final determination.

2. Terminated. An investigation is indicated as terminated when the investigation is ended for some reason other than completion, e.g., withdrawal of the request for investigation, transfer of investigative jurisdiction, etc.

3. Suspended. An investigation is indicated as suspended when the findings are inconclusive and all tangible leads have been exhausted, yet there remains a possibility that new information will be available at some future time.

4. Pending. An investigation is indicated as pending when the investigation is continuing.

(b) Block 23, the Synopsis, is written in a narrative style and contains the essence of the pertinent information in the collected Agent Reports. It is a concise summary of the who, what, when, where, why, and how of the investigation. Each statement of fact in the synopsis contains parenthetical references to the appropriate numbered Agent Reports or exhibits. Any recommendations, reviewer's opinions, or conclusions deemed appropriate should be noted on the letter of transmittal accompanying the Report of Investigation; no such comments should be included in the Report of Investigation. The margins will be the black lines at the sides of the page, and the text will begin on the third line of block 23. Two blank spaces are left at the bottom of the page. If additional space is needed, block 23 will be continued on a plain sheet of white bond paper, using normal margins. At the top of the continuation sheet the title will be placed on the left and the date and file reference on the right. The text is continued on the third line below the file reference. (See AR 381-130 for the distribution of the Report of Investigation.)
**REPORT OF INVESTIGATION**

*(Background or Complaint)*

**SCOPE (If background)**

<table>
<thead>
<tr>
<th>LAC</th>
<th>GAC</th>
<th>PBI</th>
<th>CBI</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**CASE CLASSIFICATION**

| DATE SUBMITTED | 1 April 1971 |

**IDENTIFYING DATA**

| 1. LAST NAME - FIRST NAME - MIDDLE NAME | BROWN, Margaret, Nee: ROE |
| 2. SVC NO. (Wt) | 207-24-3003 |
| 3. RACE | Cau |
| 4. GRADE | Captain |
| 5. ARM OR SVC | WAC |
| 6. DUTY OR JOB ASSIGNMENT | Administrative Asst, S4 Section |
| 7. DATE OF BIRTH | 10 June 1920 |
| 8. PLACE OF BIRTH | Nashville, Tennessee |
| 9. DUTY STATION OR BUSINESS ADDRESS | Stockton Ordnance Depot, California |
| 10. HOME OR QUARTERS ADDRESS | 1526 Center Street, Stockton, California |
| 11. TITLE OF INCIDENT (Fire, explosion, etc.) | N/A |
| 12. DATE (Incident case only) | N/A |
| 13. TIME (Incident case only) | N/A |
| 14. LOCATION (Installation, unit, building) | N/A |
| 15. SERIAL NUMBERS OF EQUIPMENT, TANKS, ETC. | N/A |

**CONTROL DATA**

| CONTROL SYMBOL AND FILE NO. | 207-24-3003 |
| INVESTIGATIVE DATA | 115th MI Group |
| INVESTIGATION MADE BY (Organization) | US Army Intelligence Command, Fort Holabird, Maryland |
| 20. REASON FOR INVESTIGATION | To determine whether SUBJECT is or ever was a member of an organization inimical to the United States, or in sympathy with such an organization. |
| 21. DATE INVESTIGATION COMMENCED | N/A |
| DATE INVESTIGATION COMPLETED | N/A |

**STATUS**

<table>
<thead>
<tr>
<th>CLOSED</th>
<th>TERMINATED</th>
<th>SUSPENDED</th>
<th>PENDING</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**SYNOPSIS**

BROWN was born on 10 June 1920 in Nashville, Tennessee (1, 2). From 1937 to 1941, SUBJECT attended the University of Kentucky, Lexington, Kentucky (2). During HER senior year at the university, SHE wrote a paper in which SHE voiced strong Marxist sentiments (3). In 1941, SUBJECT married William Roger Brown, a University of Kentucky instructor. The Brown residence became a center of leftist activities at the university. In 1942, BROWN’S husband was dismissed from the faculty of the University of Kentucky because of Communist activities and propagandism (3, 4, 19, 20).

In 1942, BROWN moved to New York, New York, with HER husband who was appointed an assistant professor at New York University. In 1943, BROWN’S husband left his position at New York University to devote his entire time to Communist propaganda activities (5, 19, 20). SUBJECT'S ideas marked HER as a militant Communist, and in 1943, SHE was issued Communist Party Membership Card No. 6794WE (7). BROWN was a secretary of a Communist front organization and an active member of many Communist

**DISTRIBUTION**

3 - CG, Sixth US Army, 1 - File

**REVIEWED BY**

| TYPE NAME AND TITLE | ROBERT C. HALL, Colonel, GS, G2 |
| SIGNATURE | /s/ Robert C. Hall |

**Figure B-8. Example of an ROI.**
sponsored groups (8, 18, 19). In 1944 BROWN made a speech in which SHE berated labor "for playing into the hands of the capitalists" (6). According to a neighbor SUBJECT and HER husband entertained frequently in their home, but these occasions were quiet and reserved. This neighbor described SUBJECT as friendly and patriotic(11).

In March 1944, when SUBJECT's husband was inducted into the US Army, he listed his political affiliations as "Communist." In December 1945, he was discharged at Fort Dix, New Jersey (12). One year after HER husband's discharge, BROWN joined the WAC in the grade of second lieutenant. SHE is currently assigned duties at the Stockton Ordnance Depot (13, 14, 15). SUBJECT's Commanding Officer and four co-workers noticed no manifestations of left-wing activity or of sympathy for left-wing causes on the part of BROWN (13, 14, 15, 16, 17). BROWN's name appeared on a membership list of the National Committee for Human Welfare, a Communist front organization (EXHIBIT I) (18, 25). In 1958, BROWN's daughter, a Communist Party youth director in Stockton, married a suspected Communist Party organizational leader (20). The Browns receive Communist literature at their home in Stockton (8, 21). They have corresponded or spoken on the telephone with three recognized Communists (22, 23, 24).

NOTE: a. Items 1 through 21 are self-explanatory.
b. The appropriate term of the "status" block (Item 22) always must be checked.
c. Plain bond used for continuation page.

Section IV. SUMMARY OF INFORMATION (DA FORM 568)

B-9. Format and Preparation
A Summary of Information should contain concise statements of both derogatory and favorable information so that the perspective will not be distorted. Rules relative to the preparation of a Summary of Information are as follows (fig B-9):

a. The date of preparation and the preparing office must be recorded in the appropriate spaces. A file number, if appropriate, may be entered in
the extreme right portion of the space labeled "preparing office."

b. The subject of the summary must be identified as thoroughly as possible. Rules for completion of the subject block for the Agent Report also apply for the Summary of Information.

c. The text of the Summary of Information will start on the third line from the black line at the top of the block titled "Summary of Information," leaving two blank spaces at the top of this block. The black lines will be used as the left margin for all items.

d. Paragraphing and subparagraphing should follow the rules of military correspondence (AR 340–15). Paragraphs are numbered at the time of preparation. Each paragraph should be limited to information from one major source only (i.e., one file, one agency, etc.), but not necessarily from one ultimate source (i.e., each person interviewed, each report of a records check, etc.), and should contain all information from that source pertinent to the subject of the Summary of Information.

e. Each paragraph of the Summary of Information will be evaluated, using the standard system of evaluation ratings (FM 30–5), taking into consideration the evaluation(s), if any, of the original report(s). When pertinent, evaluation should be made of subparagraphs or sentences.

f. If additional space is needed, two lines will be left at the bottom of the form, and the text will be continued on a plain sheet of white paper; normal margins will be used. At the top of the continuation sheet the subject will be placed on the left side and the date and file references on the right; the text is continued on the third line below these items.

g. The Summary of Information is not signed; however, the file copy will have the name of the individual who prepared the summary typed in the upper-right hand corner of the DA Form 568.

B–10. Limitation on Identification of Sources

The sources of information normally should not be revealed in a Summary of Information sent outside intelligence channels. However, if the summary is to remain in intelligence channels, the source may be identified in such identification is necessary for complete understanding of the facts. When the source is not identified, an indication of the nature of the source's accessibility to the information may be included in the summary. When Summaries of Information are prepared in which sources are not identified, the file copy which remains in the office of origin should be annotated to show the sources, using code number of sources whose identity requires protection. A bibliography may be attached to the file copy when multiple sources are used in the preparation of the Summary of Information.

B–11. Information from Other Government Agencies

Information obtained from government agencies other than the Department of Defense will not be included in Summaries of Information prepared for a requesting or receiving agency outside of the Department of Defense or the Federal Bureau of Investigation without first securing the approval of the originator or source. When a Summary of Information contains information from other government agencies, such information will be underlined and capitalized. Such Summaries of Information will contain the following statement:

Information derived from sources other than Army Sources is included in this summary. This information will not be passed to any agency outside the Department of Defense or the Federal Bureau of Investigation.

This statement will appear as a final, but unnumbered, paragraph in the summary.

B–12. Format and Preparation

A Summary of Information could be used as a characterization; however, many occasions arise where a biographic sketch of an individual or organization will satisfy the needs of the requester. Characterizations may be prepared from existing records in the US Army Investigative Records Repository, the Office of the Assistant Chief of Staff for Intelligence, DA, or the Federal Bureau of Investigation. If not available from these sources the information will only be obtained through authorized liaison with local, state, and federal authorities, and from public sources, such as reputable news media or libraries (fig B–10, B–11, B–12).
SUMMARY OF INFORMATION

HEADQUARTERS, US ARMY INTELLIGENCE COMMAND, Fort Holabird, Maryland 21219

PREPARING OFFICE

15 March 1972

SUBJECT: DOE, John Joseph
DPOB: 3 August 1936, Hometown, AZ
SSAN: 216-52-3724

CODE FOR USE IN INDIVIDUAL PARAGRAPH EVALUATION

OF SOURCE:

COMPLETELY RELIABLE ... A
USUALLY RELIABLE ... B
FAIRLY RELIABLE ... C
NOT USUALLY RELIABLE ... D
UNRELIABLE ... E
RELIABILITY UNKNOWN ... F

OF INFORMATION:

CONFIRMED BY OTHER SOURCES ... 1
PROBABLY TRUE ... 2
POSSIBLY TRUE ... 3
DOUBTFULLY TRUE ... 4
IMPROBABLE ... 5
TRUTH CANNOT BE JUDGED ... 6

SUMMARY OF INFORMATION

1. On 1 March 1972, a source who has provided reliable information in the past reported the following: On 28 February 1972, John Joseph DOE, DAC, 1969 Tucson Avenue, Bisbee, AZ, had dinner with Alex A. Smith in the Longhorn Restaurant in Douglas, AZ. The two men ate quietly in an isolated part of the restaurant and exchanged several pieces of paper before departing company. They were together from 1700-1900 hours.

2. Investigative reports concerning Alex A. Smith on file at this headquarters revealed the following: Smith was born on 28 October 1930, in Portland, ON. He was graduated from Central High School in 1949, and then attended the University of California at Berkley, where he was graduated magna cum laude in 1953 with a degree in international affairs. He has been an active sympathizer with the Communist Party, USA. He was drafted into the U.S. Army in June 1953. Throughout his term of service in the Army, Smith was known as an agitator, trouble-maker, and Communist sympathizer. Basing his actions upon minor or imaginary grievances against military service, he made numerous attempts to organize protest meetings among military personnel. (Information concerning Smith's Army activities was obtained in ten interviews with members of his military unit. Sworn statements attesting to these activities are filed at the US Army Investigative Records Repository, Fort Holabird, Maryland 21219.) Smith received a general discharge in January 1955. Smith is considered unacceptable for further military service. Smith has been living in Mexico since 1970 following federal charges of destruction and theft of government property.

3. An investigative report concerning John Joseph DOE on file at this headquarters revealed the following: DOE was born on 3 August 1936, in Hometown, AZ. HE attended Hometown High School from 1951 to 1955 and was graduated as salutatorian of HIS class. After graduation, HE attended World Electronics School in Chicago, Illinois for two years. HE then applied and was accepted for a job with the Fort Huachuca Communications-Electronics Agency. Throughout the Vietnam War HE expressed strong opposition to the War on the grounds that the American involvement in Indo-China was for territorial gain. He is suspected of having aided U.S. Army deserters in their flight to Canada.

4. A source considered to be usually reliable reported that in February 1972, DOE applied for a sensitive position with another government agency.

Information derived from sources other than Army sources is included in this summary. This information will not be passed to any agency outside the Department of Defense or the Federal Bureau of Investigation.

DISTRIBUTION

Tucson Office, FBI, Tucson, AZ - 2 copies
File - 1 copy

Figure B-9. Example of an SOI.
**SUMMARY OF INFORMATION**

**PREPARING OFFICE**
HEADQUARTERS, US ARMY INTELLIGENCE COMMAND, Fort Holabird, Maryland 21219

**SUBJECT**
NOMAN, Raffel D.
DPOB: 30 February 1900, City, Utah
SSAN: 100-00-000

**CODE FOR USE IN INDIVIDUAL PARAGRAPH EVALUATION**

<table>
<thead>
<tr>
<th>OF SOURCE:</th>
<th>OF INFORMATION:</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMPLETELY RELIABLE</td>
<td>CONFIRMED BY OTHER SOURCES.</td>
</tr>
<tr>
<td>USUALLY RELIABLE</td>
<td>PROBABLY TRUE.</td>
</tr>
<tr>
<td>FAIRLY RELIABLE</td>
<td>POSSIBLY TRUE.</td>
</tr>
<tr>
<td>NOT USUALLY RELIABLE</td>
<td>DOUBTFULLY TRUE.</td>
</tr>
<tr>
<td>UNRELIABLE</td>
<td>IMPROBABLE.</td>
</tr>
<tr>
<td>RELIABILITY UNKNOWN</td>
<td>TRUTH CANNOT BE JUDGED.</td>
</tr>
</tbody>
</table>

**SUMMARY OF INFORMATION**

1. Raffel D. NOMAN, born 30 February 1900, City, Utah, retired from the US Army in 1952, with rank of Colonel, NOMAN was decorated for his service in World Wars I and II.

2. NOMAN is a legitimate collector of autographs and photographs, especially from prominent military, political and industrial persons.

---

**Figure B-10. Example of a characterization—individual, SOI format.**
SUMMARY OF INFORMATION

DATE
15 March 1977

PREPARING OFFICE
HEADQUARTERS, US ARMY INTELLIGENCE COMMAND, Fort Holabird, Maryland 21219

SUBJECT
RETREAT COFFEE HOUSE
200 Rollybird Avenue
Baltimore, Maryland

CODE FOR USE IN INDIVIDUAL PARAGRAPH EVALUATION
OF SOURCE: OF INFORMATION:
COMpletely RELiABLE .... A AND CONFIRMED BY OTHER SOURCES... 1
USuALLy RELiABLE .... B PROBably TRUE .... 2
FAIRLy RELiABLE .... C POSSibly TRUE .... 3
MOT UsuALLy RELiABLE .... D DOUBTFLy TRUE .... 4
UNRELiABLE .... E IMPoBABLE .... 5
RELiABILITY UNKNOWN .... F TRUTH CANNOT BE JUDGED .... 6

SUMMARY OF INFORMATION

1. The RETREAT COFFEE HOUSE (RCH), 200 Rollybird Avenue, Baltimore, Maryland, opened 28 February 1977, to provide a meeting place for dissident military personnel in the Baltimore and surrounding area. RCH was organized by the No Military Action Group (NMAG), a corporation which has established coffee houses near major US Army installations for the purpose of generating and supporting military dissidence.

2. Although the RCH management staff is composed entirely of civilians, the patronage of RCH is entirely military. Approximately 30-40 individuals reportedly attend SUBJECT nightly.

3. Activities at RCH center around "rap sessions" and military counseling. Trained counselors, both civilian and military, advise and assist servicemen to seek service discharges on grounds of conscientious objector status. RCH patrons discuss and plan a variety of disruptive actions against the Army.

Figure B–11. Example of a characterization—organization, SOI format.
PERSONALITY CHARACTERIZATION

Dossier No:
As of Date:

1. NAME:  
   DPOB:  
   ASN:  
   SSAN:  

2.Aliases:

3. Marital Status:

4. Current Residence:

5. Current Employment:

6. Education:

7. Previous Residences:

8. Previous Employment:

9. Military Service:

10. Arrest Record:

11. Foreign Travel:

12. PHYSICAL DESCRIPTION
   SEX:  
   RACE:  
   HEIGHT:  
   WEIGHT:  
   EYES:  
   HAIR:  
   OTHER:  

PHOTOGRAPH AS OF:

POLITICAL AND ORGANIZATIONAL ASSOCIATIONS
AND AFFILIATIONS

OTHER INFORMATION

Figure B-12. Example of a characterization—individual on bond paper.
APPENDIX C
COUNTERINTELLIGENCE SERVICES REPORTS


EXAMPLE 1
REPORT OF COUNTERINTELLIGENCE SURVEY
OF
(UNIT AND LOCATION)

( Requester Control Number) (Date)

Section I. INTRODUCTION
1. A counterintelligence survey was conducted (during the period ______
to __________) or (on __________) by the following representative(s) of (Region ______), (______) Military Intelligence Group:

(List as necessary using title, first name, middle initial, and last name.)

2. The following unit representatives accompanied the counterintelligence survey team:

(List as necessary using rank or title, first name, middle initial, last name, and position.)

3. (Indicate whether or not there is any record of a previous counterintelligence survey having been conducted on the above installation.)

4. The mission of (identify the surveyed unit completely) is (discuss briefly the complete mission of the surveyed unit).

5. Based on the factors discussed below (maximum, medium, minimum) degree of security is required for the surveyed unit.

a. (Discuss effect of the mission of the surveyed unit on the level of security required.)

b. (Statement of cost of replacement.)

c. (Briefly discuss location of the installation.)

d. (Give number and names of like installations.)

e. (State the security classification of information and/or materiel.)

f. (Discuss other factors relating to the overall importance of the surveyed unit.)

6. Command directives for this installation are promulgated by (enter identification of surveyed unit's major command) through (enter command echelons, if any, between major command and surveyed unit). The intelligence directives are disseminated to this installation by (enter source of directives) through (enter the intelligence echelons, if any, between major command and the surveyed unit).

7. This survey was conducted to assist the commander in establishing the security requirements necessary to protect his installation against espio-
nage, sabotage and the unauthorized access to, or disclosure of, classified defense information.

Section II. SCOPE

8. This survey included the following (elements, offices, sections, etc) of (re-identify the unit).

(List the sections or sub-elements surveyed.)

9. (Use this paragraph to indicate the amount and classification of documents and materiel on hand either by number and type or in linear feet and type.)

Section III. FINDINGS AND RECOMMENDATIONS

10. Security of Information:

a. Receipting: (Narrate the entire procedure used in receipting for all classified documents within the unit being surveyed and follow with appropriate recommendation(s). An alternate method would be to subparagraph where required, as in example below.)

(1) TOP SECRET: (Narrate)

(a) Recommendation: (Follow the narration with appropriate recommendation(s). Use a similar procedure for subsequent paragraphs throughout the report, varying as necessary to adapt survey findings to this report format.)

(b) Recommendation:

(2) SECRET: (Narrate)

(a) Recommendation:

(b) Recommendation:

(c) Recommendation:

(3) CONFIDENTIAL: (Narrate)

(a) Recommendation:

(b) Recommendation:

b. Storage. (Narrate in detail facilities and procedures employed in storing classified matter.)

Recommendaion(s)

c. Distribution: (Narrate in detail procedures employed for internal distribution of classified matter.)

Recommendaion(s)

d. Preparation: (Narrate in detail how classified matters are generated and prepared, to include drafts.)

Recommendaion(s)

e. Marking: (Narrate in detail how prepared classified matters are marked for proper safeguarding, to include drafts, stenographer's notes, etc, and also authority.)

Recommendaion(s)

f. Reproduction: (Narrate in detail how classified matters are reproduced and how marked.)

Recommendaion(s)

g. Regarding: (Narrate in detail procedure for reviewing and regrading classified matter; include responsibility.)
Recommendation (s)

h. Transmission: (Narrate in detail procedure employed for transmitting classified matter out of the surveyed unit to include responsibility and accountability.)

Recommendation (s)

i. Normal Destruction: (Narrate in detail procedure employed for accomplishing normal destruction of classified matter and waste; include responsibility, records, etc.)

Recommendation (s)

j. Emergency Evacuation and Destruction of classified material: (Narrate in detail what measures are established to include plan in effect, personnel assigned specific duties, etc.)

Recommendation (s)

11. Security of Personnel:

a. Key Personnel:

(1) The (enter title of individual who heads the surveyed unit; i.e., commanding officer, branch chief, section chief, etc.) of the installation is (enter title or rank, first name, middle initial, last name, branch of service, service, social security number or GS rating in case of civilians). He (or she) has occupied this position since (date).

(2) The Security Officer of this installation is (enter title or rank, first name, middle initial, last name, branch of service, social security number or GS rating in case of civilians). He has occupied this position since (date) upon orders issued by (identify authority and date).

(3) The officer having staff responsibility for crime prevention at this installation is the Provost Marshal (or appropriate title), (enter rank, first name, middle initial, last name, branch of service, and social security account number). He has occupied this position since (enter date) upon orders issued by (identify authority and give date of orders).

(4) (Use additional subparagraphs, as needed, to identify other individuals in surveyed unit who are considered to be “key” personnel and show the degree of clearance and time each has held his present position.)

Recommendation (s)

b. Clearance Program: (Describe in detail the procedure used for obtaining clearance for assigned personnel and describe accuracy of the clearance roster.)

Recommendation (s)

c. Security Education: (Describe in detail the security education program that is established and conducted; include responsibility, frequency of security lectures, subjects covered, attendance records, effectiveness, etc.)

Recommendation (s)

d. Labor Turnover, Absentee Rate, Morale: (Describe how these factors affect the security of surveyed unit.)

Recommendation (s)

12. Physical Security: (Describe in detail the controls, systems, facilities, and utilities identified in the following subparagraphs. If the unit being surveyed already has on record a Physical Security Survey (PSS) performed by MP personnel, a statement in this paragraph referring to the report is deemed sufficient, provided those deficiencies noted which directly
affect the security of classified documents and material have been corrected. If this has not been accomplished, appropriate recommendations should be made. If there is no record of a PSS and the MP representatives are unable to perform the physical security portion while the CI Survey is being conducted, this portion will be accomplished by counterintelligence personnel, if directed to do so, following the format outlined below (chap 10).

a. Perimeter Barriers:
   - post: fences, gates, locks, key control, perimeter lighting;
   - building: building surfaces, doors, locking devices, key control, windows, protective lighting;
   - office: wall surfaces, doors, locking devices, key control windows.

Recommendation(s)

b. Guards and Guard Systems:
   - post: type and number of guards, their procurement training, their employment and supervision, equipment and communications;
   - building: same as above;
   - office: same as above.

Recommendation(s)

c. Personnel Control and Identification: Control of assigned personnel by post, in building, and in office; control of visitors by post, in building, and in office.

Recommendation(s)

d. Vehicular Control and Identification: Vehicles of assigned personnel, their registration, identification and control on post; visiting vehicles and their control.

Recommendation(s)

e. Anti-Intrusion Alarms Systems:

Recommendation(s)

f. Firefighting Facilities:
   - post: fire department and its personnel, type and number, procurement and training, employment and supervision; equipment and its inspection; communications; reserve fire fighting personnel;
   - building: fire plan; fire marshal and wardens, equipment and its inspection; communications; training and education of personnel;
   - office: same as for building.

Recommendation(s)

g. Communication Facilities: Primary, alternate, and emergency facilities that are available on post and to surveyed unit; personnel employed to operate and maintain communications facilities to include their type and number, procurement and clearance, employment and supervision.

Recommendation(s)

h. Utilities:
   (1) Electrical Power.
       (Source, emergency provisions, protection, etc.)
   (2) Water Supply.
Section IV. COMMENTS

13. (Use this section to record weaknesses and any other comments considered pertinent. As a part of the survey, inquiries into the following areas will also be made and if they are found to be adequate, appropriate remarks to that effect will be made in this section.

a. An evaluation of the completeness and correctness of the unit's security SOP.

b. Examination of sensitive areas, classified conference rooms and potential or actual restricted areas, to include their actual designation as such or the requirement for a counterintelligence technical service. If these areas are found to be inadequate from the standpoint of published regulations, directives, and implementation thereof, the discussion should be placed in section III, above, followed by appropriate recommendation(s). When weaknesses as described in chapter 10 are noted, discussion and recommendation(s) will appear in this section.)

Section V. EXIT BRIEFING

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

(List as necessary using rank or title, first name, middle initial, last name, and position.)

SIGNATURE BLOCK
(Signature of authorized group representative, not necessarily the Agent-in-Charge.)

EXAMPLE 2
(CLASSIFICATION)
REPORT OF COUNTERINTELLIGENCE TECHNICAL SERVICE OF
(UNIT AND LOCATION)

(Requestor Control Number) (Date)

Section I. INTRODUCTION

1. ( ) A counterintelligence technical (survey/inspection assistance) was conducted during the period _____________ by the following representative(s) of Region ___________, ( ), MI Group.

(List as necessary using title, first name, middle initial, and last name.)

2. ( ) The serviced area was considered by the requester to be a (enter secure conference facility, or other sensitive area). A description of the area is contained in EXHIBIT I.

3. ( ) An examination of records regarding previous counterintelligence technical services in the area reveal that: (check as appropriate)

   ( ) There is no record of a previous technical service.

   ( ) A counterintelligence technical (identify) was completed on
Section II. SCOPE

4. (U) The scope of this technical service is outlined in EXHIBIT II.

Section III. LIMITATIONS

5. (U) The limitations of this service are outlined in EXHIBIT II.

Section IV. FINDINGS AND RECOMMENDATIONS

6. ( ) Repeated or uncorrected findings: (enter here any repeated or uncorrected findings. If there were none, enter, none).

7. ( ) (If technical surveillance devices were not detected and no technical security hazards were found, state: "The service did not locate or indicate the presence of technical surveillance devices or technical surveillance security hazards.")

8. ( ) (If technical surveillance devices were not detected, but technical security hazards were found, state as follows:
   a. The service did not locate or indicate the surveillance devices.
   b. The serviced area does not meet the criteria for sensitive areas and is not considered secure for the discussion of sensitive classified information until corrective action is taken on the following technical security hazards:
      (1) Finding: (Record findings and follow each with an appropriate recommendation. Paragraph citations will be indicated at the end of each finding. When an appropriate finding cannot be attributed to an appropriate directive, a parenthetical caveat (NONCITABLE HAZARD) will be entered at the end of such findings.)
      (2) Finding: (Recommendation:)

Section V. COMMENTS

9. ( ) (Use this section to record any additional pertinent explanatory remarks that do not properly fit into any of the other sections).

Section VI. EXIT BRIEFING

10. ( ) All findings, recommendations, and limitations of the service were discussed during an exist briefing on __________ for the following unit representatives:
    (List as necessary using rank or title, first name, middle initial, last name, and position.)

SIGNATURE BLOCK
(Signature of authorized group representative, not necessarily the Agent-in-Charge.)

REPORT OF COUNTERINTELLIGENCE TECHNICAL SERVICE
OF
DESCRIPTION OF SERVICED AREA

1. ( ) Primary use of serviced area-highest classification and frequency of discussion of classified defense information.
   (CLASSIFICATION)
SCOPE OF TECHNICAL SERVICE

1. (U) Unless otherwise indicated, this service was conducted to detect the presence of technical surveillance equipment; to determine the existence of technical security hazards which would permit the employment of such equipment; and to recommend technical security measures designed to prevent the successful employment of technical surveillance monitoring systems.

2. ( ) This service consisted of selected application of comprehensive visual, physical, audio, electronic, and radio frequency checks and included an examination of the factors checked below:

   ( ) a. All exterior building surfaces, utility poles, wires, and other associated paraphernalia.
   ( ) b. Vulnerability of hostile visual surveillance.
   ( ) c. All areas adjacent to the serviced area including those areas above and below.
   ( ) d. The interior of room areas to include wall, floor, and ceiling mounted items, furniture, artifacts, and equipment.
   ( ) e. The interior and exterior surfaces and internal structure of walls, floors, ceilings, and other structural objects.
   ( ) f. All electric or electronic equipment or circuits and component parts of accessories thereof, to include detailed examination of all wiring and utility channels or recesses.
   ( ) g. Other:

LIMITATIONS OF TECHNICAL SERVICE (U)

Counterintelligence technical services of the type conducted indicate the technical security status of the area or equipment examined at the conclusion of the examination, within the capabilities of the equipment utilized and the operational techniques employed. Attention is invited to the fact that the security afforded by this service WILL BE IMMEDIATELY NULLIFIED BY:

   a. Admission to the serviced area of persons who do not have the proper security clearance or who are not under proper escort.
   b. Failure to maintain continuous and effective surveillance and control of the serviced area.
(CLASSIFICATION)

c. Allowing repairs or alterations to or within the serviced area without the supervision of qualified and responsible personnel.

d. The introduction of new furnishings or equipment into the serviced area prior to a thorough inspection of such items.

e. Other limitations:

EXHIBIT II

Page 2
APPENDIX D
COUNTERINTELLIGENCE SURVEY CHECKLIST

Note. The Provost Marshal’s role in security is related to the prevention of unauthorized entry, control of entry, circulation and exit of personnel and vehicles, perimeter barriers and approach areas, protective lighting and alarm systems, pass and badge systems, and prevention and detection of crime. To accomplish this responsibility, Physical Security Surveys (PSS) are conducted periodically by Military Police personnel. A copy of a PSS may be attached to the report of counterintelligence survey, and appropriate references to the PSS should be incorporated into the report. When the time lapse is extensive, or when there is no record of a prior PSS, arrangements should be made to have a PSS conducted concurrently with the counterintelligence survey (chapt 10). In the event that this is not possible, FM 19-30, contains a checklist that should be used by counterintelligence personnel conducting the physical security portion of the survey.

Section I. PRELIMINARY CHECK

D–1. Topography
Check the natural topographic features existing at the periphery of the installation.

a. Determine whether these natural features have an adverse effect on the security of the installation. Explain.

b. Determine whether these features can be utilized as deterrents to unauthorized entry. What additional physical security measures are necessary for these features to be of value as barriers?

c. Determine whether potential intruders or espionage/sabotage agents can utilize these topographic features as possible cover and concealment. What measures are necessary to deny use of these features by potential intruders?

D–2. Surrounding Area

a. Check the population surrounding the installation to determine whether there is any aspect that would have an adverse effect on the security of the installation.

(1) Determine the ethnic derivation of the population. Do these people present any threat to the security of the installation?

(2) Determine whether there are any racial problems. Will racial riots have adverse effects upon the security of the installation?

(3) Determine whether any group favors ideologies not consistent with the best interest of the United States or of the nations with which the US enjoys an amicable relationship.

(4) Determine the crime rate. What types of crimes predominate? Do these criminal acts present threats to the security of the installation?

b. Check the area surrounding the installation for any organization which may present threats to the security of the installation. Determine whether there are any political, labor, fraternal, or social organizations which are engaged in activities inimical to the best interests of our government. Identify officials and members of such organizations. What is their platform? Are they supported by subversive organizations?

c. Check the industries essential to the function of the installation.

(1) Are any of the industries essential to the function of the installation?

(2) Determine whether strikes and riots will have adverse effects on the operations and security of the installation and how.

d. Check places of entertainment such as bars, restaurants, nightclubs located in the proximity of the installation.

(1) Determine whether these places of entertainment are frequented by personnel of the installation.

(2) Determine which of these establish-
ments, if any, are known to cater to individuals who harbor ideologies inimical to the best interests of our government.

(3) Determine whether there have been known incidents in these establishments to solicit information concerning the installation and/or its activities.

(4) Monitor establishments to determine whether military personnel discuss defense information while on the premises.

**D–3. Critical Areas**

a. Determine the locations of such critical areas as the communication centers, power transformer stations, fuel storage sites, POL dumps, and ammunition dumps.

(1) Check the measures taken to protect these areas.

(2) Determine their relationship to, and distance from, sensitive areas.

b. Determine the location of the motor pools.

(1) Check whether they are properly safeguarded. Are any areas designated for authorized personnel only?

(2) What types of vehicles are located in the motor pools? Are vehicles frequently checked for possible mechanical sabotage?

c. Determine whether airstrips and/or heliports have been established.

(1) Check whether the installation has assigned aircraft and pilots.

(2) Are aircraft properly safeguarded?

(3) Are airstrips and/or heliports clearly designated? If there are neither, determine whether there are large enough areas.

**Section II. HISTORY AND SENSITIVITY OF THE INSTALLATION**

**D–4.**

a. Examine the history of the installation.

b. Check the history of the installation as it pertains to the construction of tunnels, caves, sewers, underground facilities, entrances and exits, or any other construction that would have an adverse effect on the security of an installation.

**D–5.**

What is the mission of the installation being surveyed? Is it classified or unclassified, and is it of long or short duration? How does the mission contribute to the defense effort? Is the mission extremely sensitive or nonsensitive?

**D–6.**

Determine the cost of replacement.

a. What would it cost in terms of money, manpower, material, and time to replace this installation if it were destroyed?

b. How would this affect the defense effort?

(3) Determine whether these areas have been designated as restricted areas or off-limits areas.

**D–7.**

Consider the vulnerability of the location of the installation and what effect the surrounding elements have upon its security, based on factors developed in section I above.

**D–8.**

Consider the classification of the information stored, used, and created at the installation.

**D–9.**

Determine the number of like installations that are capable of absorbing the functions of the surveyed installation if it were destroyed.

**D–10.**

Determine the overall importance of the installation commander and examine higher command or DA policy to establish a partial basis for the determination. Evaluate items in paragraphs 4 through 9, above. It is extremely important that this determination be made prior to the survey so that feasible recommendations may be rendered.
Section III. SECURITY OF INFORMATION

D—11. Amount of Classified Documents and Material

How many linear feet of each category of classified information are stored in the surveyed installation?

D—12. Message Center

Is a message center used for distribution of all incoming correspondence and dispatch of all outgoing correspondence? If so:

a. How many personnel are employed in the message center?

b. In relation to the classification of information handled, are the message center personnel adequately cleared?

c. Is the message center declared a Restricted Area? If so who is authorized access? What identification system is used?

d. What storage facilities are available in the message center?

f. How much information of a classified nature is stored in the message center?

D—13. Storage Facilities

a. How are SECRET and CONFIDENTIAL materials stored? Describe the containers to include size, weight, type of locking device, and approximate delay time.

b. If containers with steel locking bars and hasps are used (as an interim measure until required containers are received), are the hasps adequately secured to the containers? Are the locking bars attached to the containers in such a way that material cannot be removed from the drawers when the container is locked?

c. If a field safe is used for storage, is it secured to the building or guarded to prevent unauthorized removal? Describe the safe and locking device.

d. When, or under what circumstances, are combinations to combination locks used on classified containers changed?

e. Is an up-to-date record of all safe combinations maintained in a central location, together with information necessary to identify and locate all containers? If so, where? Who has access to the combinations? Are the combinations afforded protection as required for at least the highest category of information in any of the containers? Consider the overall classification of a compilation of the material that would be available to anyone gaining access to the record of combinations.

f. Has the dissemination of combinations been held to the minimum consistent with efficient operations? Explain.

g. Is a properly completed part 1 of DA Form 727 (Classified Container Information) affixed to the outside of each container in which classified information is stored? Check for accuracy.

h. Are all personnel listed on part 1 of DA Form 727 currently responsible for the security of the container on which the form is posted?

i. Is part 2 of DA Form 727 properly executed and attached to an envelope containing the combination recorded on part 3 of DA Form 727? Have these been filed in a central location at the next higher echelon? Where?

j. Is part 3 of DA Form 727 placed in an opaque envelope? Is it possible to read the combination through the envelope? Is the envelope sealed?

k. Is part 3 of DA Form 727 classified at least as high as the highest category of defense information stored in the container? Consider the need for a higher classification due to the effect of a compilation of the information in the container.

l. Is the envelope containing part 3 of DA Form 727 marked with the same classification as the form inclosed?

m. What procedure is followed to insure that combinations are not written on calendar pads or carried in wallets?

n. Is a properly executed DA Form 672 (Safe or Cabinet Security Record) affixed to each container in which classified information is stored? Check for accuracy. (Note any discrepancies found on DA Form 672.)

o. Is an entry made on DA Form 672 each time the container is opened and closed? Do the initials in the "UNLOCKED BY" column coincide with the names listed on part 2 of DA Form 727 as having knowledge of the combination?

p. Is the person who checked the container at
the end of the day different from the person who locked the container?

q. Is the container checked every working day, even if it has not been opened?

r. If a container remains open, is it attended by a properly cleared, responsible person? Explain.

s. When a container equipped with combination padlock (interim arrangement) remains open during duty hours, how is the padlock safeguarded?

t. Are containers in which classified information is NOT to be stored clearly marked with instructions to this effect if prescribed by local security SOP? Explain.

u. Are personnel aware of the action required when a container is found open and unattended after duty hours or classified material is found unattended and out of a container? Query personnel and report results.

v. When removed from the installation is classified material kept under personnel physical control of authorized personnel at all times or secured in the type of storage facility required by the particular classification?

w. How is information annotated “FOR OFFICIAL USE ONLY” stored?

x. Are NATO, CENTO, or SEATO documents clearly identified and segregated from US documents in storage?

D—14. Classified Document Register

a. Is a classified document register maintained for classified material charged to the unit surveyed? (Dependent on local policy, a register may or may not be maintained for CONFIDENTIAL and SECRET material.) Describe the register utilized for such material.

b. Does the register bear an overall classification based on the presence of classified information contained therein rather than on the presence of references to classified information? Spot check for accuracy.

c. Are individual pages of the register classified according to the classification of long titles contained thereon? Spot check for accuracy.

d. Do the entries fully identify the documents? Cross check the register entries with documents.

e. Who is responsible for maintaining the register? Who has access to the register?

f. Does the register indicate how documents entered therein were disposed of (receipt, dispatch, downgrading, destruction)?

g. Is the register current and accurate? Spot check 5 to 20 percent of the documents entered.

h. Are all documents originated by the unit entered in the register and is there disposition indicated?

D—15. Receipting

a. Is SECRET material, CONFIDENTIAL material, if required (local policy will dictate procedure), covered by a receipt? Explain the system used.

b. What receipt form is used? Is a file copy retained for all classified documents sent out of the unit?

c. Is the unit making proper use of DA Forms 681 (Classified Multiple Document Receipt or Tracer), 1203 (Classified Document Mail Control Record and Receipt), and 1204 (Classified Document Receipt and/or Tracer)? Explain.

d. Do receipt forms contain any classified information? Spot check.

e. If all receipt forms have not been returned for documents sent out of the unit, have they been traced through use of proper forms? Report results of any tracers sent out since the last survey of inspection.

f. Are receipt forms being disposed of in accordance with AR 340–18-series (file # 504–08) or AR 340–2 (file # 501– )? Explain.

g. Who is designated to receipt for classified material that is received by surveyed units?

D—16. Dissemination

a. Are supervisory officials taking proper steps to prevent unauthorized dissemination of classified information? Explain.

b. Is a conscious effort made by holders of classified documents to insure that requesters have proper clearance and a bona fide need-to-know?

c. Do requesters of classified information insure that they have a proper clearance and actually need the information in the performance of their official duties?

d. Are classified document cover sheets used to cover classified documents when they are out of containers and not being used?
e. How are requirements for safeguarding certain documents from foreign nationals being implemented?

f. Is classified material removed from containers at night for work purposes? If so, what provisions for proper safeguarding are in effect?

g. Are individuals within the unit required to leave a receipt for classified information they remove from containers? If so, what receipt form is used? Who controls the documents within the various offices of the unit?

D–17. Preparation of Reproduction

a. Is any classified material originated in the unit surveyed? If so, do responsible officials have written authority to classify? Include details.

b. Are persons using, extracting from, reproducing, incorporating, or responding to information already classified, carrying out their obligations to apply the classification decisions determined by the originating authority? Explain.

c. Are documents classified according to their own content?

d. Are cotton, rayon, silk, and paper typewriter ribbons properly handled when used to prepare classified material? How?

e. Are stencils containing classified information properly handled? How?

f. If Verifax, Thermo-Fax, or photostatic reproducing processes are used for classified information, what precautions are taken to insure that master copies, negatives, waste, etc. are properly protected?

g. If a printing press is used for reproducing classified material, how are matrices, master copies, excess copies, waste, etc., protected from unauthorized disclosure?

h. What protective measures are in effect to insure that carbon paper used in preparing classified information is properly stored and protected?

i. Are drafts of documents containing classified information properly protected? Explain in detail.

D–18. Transmission

a. Is classified material transmitted outside the unit surveyed? If so, what methods of transmission are used? (Mail, courier, Armed Forces Courier Service, State Department?)

b. What receipt form is used? How are documents accounted for while in transit?

c. If classified material is mailed, is the double envelope system properly used? Is a file of Post Office Department Registry receipts maintained?

d. If a courier is used to transmit classified material, does he have a clearance at least as high as the information entrusted to him?

e. Is the classified material adequately protected from view when carried by the courier? How?

f. How is material prepared for transmittal by Armed Forces Courier Service or State Department diplomatic pouch?

D–19. Classification and Marking

a. Do files or groups of physically connected documents bear the overall classification of the highest classified components? Consider the effect of a compilation on the overall classification.

b. Are letters of transmittal classified as high as the highest classified inclosure? If the letter of transmittal contains no classified information, are regarding instructions included?

c. Are extracts or portions of classified documents properly marked with the security classification? Spot check.

d. Is the defense classification of paragraphs, sections, chapters, indorsements, annexes, inclosures, subjects or titles properly indicated? Spot check.

e. Is the defense classification of documents properly indicated? Spot check.

f. Are documents and paragraphs containing RESTRICTED DATA or FORMERLY RESTRICTED DATA properly marked? Spot check.

g. Do the prescribed special handling notices appear on documents that must not be released to foreign nationals? Spot check.

h. How are photographs, films, recordings, charts, maps and drawings containing classified information marked?

i. How is the classification indicated on material, products, or their containers?

j. How is material for training purposes marked? Spot check.
k. Do all reproductions of classified material bear the same markings as the original? Spot check.

l. Are transmittals of investigative reports containing counterintelligence information annotated in accordance with AR 381-130 if transmitted outside intelligence channels? Spot check.

D–20. Regrading and Declassification

a. What procedure is being used for prompt review of all classified documents for regrading purposes?

b. Are regrading instructions placed on all classified documents?

c. How are holders of classified documents informed of nonautomatic regrading instructions?

d. Have documents been properly regraded according to the automatic or nonautomatic regrading instructions? Spot check 5 to 20 percent of the documents on hand.

e. Do regraded or declassified documents bear proper authentication when required? Spot check.

f. If the unit has regraded or declassified original document, are recipients of the original distribution notified? How?

g. How is authority obtained for regrading documents deemed incorrectly classified?

h. How is material designated FOR OFFICIAL USE ONLY marked?

D–21. Destruction

a. Who is the person authorized to destroy classified material? Cite the authority.

b. Who is selected to serve as a disinterested witness to destruction? Is he truly disinterested? Explain.

c. Do the destruction officer and witness meet the criteria established by AR 380–5?

d. Is the witness for SECRET destruction named on orders?

e. Are appropriate records of destruction maintained? Who keeps them? Is the authority for destruction cited??

f. Cross check the certificates of destruction with the classified documents register to see that they are accurate. Does the register reflect all destructions?

g. Is a record made of destruction of CONFIDENTIAL material? Explain.

h. If a classified title is used, does the certificate of destruction bear the proper marking?

i. Note any discrepancies found in the destruction certificates.

j. How is classified material destroyed?

D–22. Emergency Plan

a. Destruction (in overseas areas).

(1) Are these provisions for emergency destruction of classified material stored by the unit surveyed? Explain.

(2) Have specific responsibilities been assigned to individuals for implementation of the emergency destruction plan? Identify the personnel. Are they aware of their responsibilities and the provisions of the emergency plan?

(3) What facilities are available for emergency destruction?

(4) Where are the collection points located?

(5) Is a system of priority marking of documents and material utilized in the unit? Explain.

b. Evacuation.

(1) Are there provisions for emergency evacuation of classified material stored by the unit surveyed? Explain.

(2) Have specific responsibilities been assigned to individuals for implementation of the emergency evacuation? Identify the personnel. Are they aware of their responsibilities and the provisions of the emergency plan?

(3) What vehicles or facilities are available for emergency evacuation?

(4) Where are the collection points located?

(5) Is a system of priority marking of documents and material utilized in the unit? Explain.

D–23. Procedure for Handling TOP SECRET

The following will apply only if the unit surveyed stores or handles TOP SECRET information or material.

a. Have a Top Secret Control Officer and an Alternate Top Secret Control Officer been appointed on competent orders? Identify them and cite the paragraph number, orders number, date, and issuing headquarters.

b. Does the Top Secret Control Officer maintain a current roster of all personnel authorized access to TOP SECRET material? Include a copy if available.

c. How is transfer of accountability accomplished upon change of Top Secret Control Officer?

d. Does the Top Secret Control Officer maintain a permanent register of DA Form 2133 (TOP SECRET Control Record) or DA Form 455 (Mail
and Document Register), as appropriate, reflecting receipt, dispatch, downgrading, or destruction of all TOP SECRET material for which he is responsible? Check all for accuracy.

e. Using the register, account for all TOP SECRET material in the unit.

f. How is the transfer or receipt of TOP SECRET material documented?

g. Are all copies of TOP SECRET documents properly numbered for accounting purposes? Explain.

h. Are results of annual inventory reported through channels to the major command or DA agency on or about 1 April each year? How is this accomplished? Check file copy(ies).

i. How is TOP SECRET material transmitted in the clear? How is it transmitted when encrypted?

j. How is the TOP SECRET material stored? Explain.

k. If a guard is used, is he properly cleared? How is he armed?

l. Does the TOP SECRET register reflect destruction of any TOP SECRET material? If so, are the number and date of the destruction certificate included?

m. How is the TOP SECRET material destroyed?

n. Who destroys the TOP SECRET material? Who witnesses the destruction? Do these personnel meet the requirements established by AR 380-5? Is the witness named on orders? Explain.

o. Is each TOP SECRET document entered individually on the destruction certificate? Are the destruction certificates serially numbered in annual series for accounting purposes? Are DA Forms 546 (Destruction of Classified Records) and 1207 (Record of Destruction for Classified Messages) used to record the destruction of TOP SECRET documents?

p. Do all TOP SECRET documents have proper instructions regarding reproduction? Is proper authority obtained prior to extracting material from a TOP SECRET document? Explain.

q. Are all TOP SECRET documents covered by a properly executed DA Form 969 (Top Secret Document Record)? Does the DA Form 969 clearly identify the document to which attached? Does the DA Form 969 reflect the names of ALL persons having access to the document and the date of such access?

(Note. Personnel on orders, such as the TOP SECRET custodian, do not have to sign the form since access is assumed.)

r. Explain in detail any discrepancies revealed in the last annual inventory of TOP SECRET material.

D–24. Procedures for Handling Registered Documents and Material

a. Has a custodian of registered documents been appointed on competent orders? Does he possess a TOP SECRET clearance? Identify the custodian and cite the paragraph, orders number, date, and issuing headquarters of the orders appointing him.

b. If an alternate custodian is appointed, include the same information as required for the custodian.

c. If there has been a change in custodians, has a transfer certificate been accomplished? Spot check.

d. Was an annual report of possession made as of 1 April? Check file copy.

e. Are references to registered documents in reports of destruction by short title, register number, and date, only? Spot check all documents.

f. Is DA Form 454 (Semiannual Inventory/Report of Transfer of non-Army Registered Documents) used for all transfers, or reports of semiannual inventory of registered documents?

g. Are the DA Forms 454 properly executed and distributed? Check all of them.

h. Is a proper receipt of DA Form 454 in the place of any registered document charged to the unit but not physically present?

i. Do all documents in which a long title appears bear a classification equivalent to the defense information contained in the long title? Spot check.

j. Are registered documents destroyed on receipt of authority from the Adjutant General?

k. Are copies of destruction certificates furnished the office of record?

l. How are registered documents stored? Must be stored according to security classification as prescribed in AR 380-5.

m. Conduct a check to insure that all pages of registered documents are physically present.

n. Did the last semiannual inventory reveal any discrepancies? If so, explain in detail.
D—25. Procedures for Handling RESTRICTED DATA
The following will apply only if the unit surveyed stores or handles RESTRICTED DATA.

a. Are semiannual physical inventories of TOP SECRET documents containing RESTRICTED DATA submitted as of 30 June and 31 December? Check to be sure.

b. What action will be taken in the event of compromise or possible compromise?

c. Are all RESTRICTED DATA or FORMERLY RESTRICTED DATA classified at least CONFIDENTIAL?

d. How are the RESTRICTED DATA documents marked?

e. Is each paragraph containing RESTRICTED DATA or FORMERLY RESTRICTED DATA properly annotated?

Section IV. PERSONNEL SECURITY

D—26. Key Personnel

a. Identify (name, rank/grade, SSN) the key personnel, to include the commander, deputy commander, and any staff officers whose functions have a direct bearing upon security. Show the degree of clearance and time each has held his present position.

b. Identify any other persons considered essential to the efficient operations of the unit, including the person’s qualifications, degree of clearance, and time in this position.

c. Identify the Installation Intelligence Officer (IIO) and the Installation Security Control Officer (SCO).

(1) Indicate the date, paragraph number, and issuing headquarters of the orders appointing the IIO and the SCO.

(2) What are the qualifications of the IIO and SCO?

(3) Do the IIO and the SCO have additional duties that tend to hinder or interfere with the performance of their duties as IIO or SCO? If so, explain them.

(4) Identify the IIO and SCO assistants, to include qualifications and time in the position.

D—27. Personnel Security Clearances Administration

a. Who maintains the roster of cleared personnel?

b. What information is included in the roster?

c. List any personnel who have access pending clearance. Indicate the degree of access and nature of their duties.

d. Who maintains certificates of clearance?

e. Are clearances properly executed on DA Form 873 (Certificate of Clearance and/or Security Determination under ED 10450)? Spot check.

f. Who executes the clearance certificates?

g. Does the person authorized to grant clearances possess a TOP SECRET clearance himself?

h. Does the “Remarks” section of clearance certificates reflect the results of any reviews conducted?

i. How frequently are clearances reviewed?

j. Is a security oath attached to each interim and final cryptologic clearance certificate?

k. What criteria or prerequisites must be met for issuance of a clearance? Spot check 5 to 20 percent of the personnel records to substantiate that appropriate investigation was conducted in accordance with AR 604–5.

l. Is a copy of the request for clearance or request for PSI maintained in the personnel records of the individuals concerned to prevent duplicate requests?

m. What system is used to insure cancellation of investigations when the SUBJECT is transferred, discharged, or for any reason has no need for a clearance?

n. Are final and interim clearances entered on the appropriate form in the individual’s personnel records? (DA Forms 20 and 66)

o. Are the clearances in accordance with existing policies and directives?

p. Are separate name files maintained on military and civilian personnel on whom investigations are pending under AR 604–10 and AR 690–1, respectively?
q. Is there a checklist or SOP to insure proper handling or processing of security risks? Describe it.

r. Are all records of military personnel considered a security risk properly flagged? Who maintains the DA Forms 268 (Report for Suspension of Favorable Personnel Action)?

s. Are the records of all newly assigned personnel screened to insure a valid DD Form 98 (Armed Forces Security Questionnaire)? Spot check.

t. Is the number of clearances in excess of the minimum consistent with the needs of the commander concerned to carry out his mission?

D—28. Security Education

Is there a formal training program for security? If so:

a. How often is training conducted? Who conducts the training?

b. What subjects are included in security training?

c. What is the average length of the training lecture?

d. Is attendance mandatory at security training lectures? How is attendance insured?

e. Is a current and correct local security policy in published form available to all personnel? Does it contain sufficient details and references? Are all personnel required to read and become familiar with the policy? How is this enforced?

f. Are security posters available? If so:
   (1) Are they adequate in number and emphasis? Where are they used?
   (2) Do the posters contain “eye appeal”?
   (3) How frequently are security posters changed?
   (4) Where are security posters produced?

g. Are personnel required to read Army Regulations pertaining to security periodically? How often? How is this enforced?

h. What type security orientation is given newly hired or assigned personnel? Who conducts this orientation?

i. What debriefing program is utilized for personnel terminating their assignment or employment?

j. Does the debriefing process incorporate positive instructions to preclude release of classified defense information to unauthorized persons?

k. Is a copy of the Attorney General’s list of organizations whose interests are in conflict with those of the United States posted conspicuously?

l. Are all appropriate personnel receiving a SAEDA orientation? (AR 381–12)

m. Are all appropriate military and DAC personnel receiving an orientation on the threat posed by, and procedure to counter, use of clandestine listening devices by hostile agencies? (AR 381–14)

D—29. Emergency Plan

Does the installation have an emergency plan with provisions for action in case of enemy attack, disaster, dispersion, evacuation, blackout, air raid, riots, or civil disturbances?

a. Are all personnel familiar with the provisions of this plan?

b. Have practice alerts been held to test the effectiveness of the plan and the proficiency of personnel in implementing it? When was the last practice alert? What were the results?

c. Is there an SOP for dissemination of air raid warning messages? Explain.

d. Are personnel familiar with this SOP and the audible air raid signal?

e. Does the emergency plan include procedures for maintaining security during an emergency?

D—30. Morale

a. Based upon interviews and observations, is there any indication of low morale? Explain.

b. If there are indications of low morale, determine the cause or source.

c. Has there been any trouble of a racial, religious, labor or political nature traceable to any source or reason of security significance? Explain.

d. Is there a labor union or organization represented by employees of the installation? If so, indicate the name and address of the local headquarters.

e. Have there been any instances which appear to involve intentional or deliberate work delays by personnel? If so, explain in detail.
f. Is a record maintained of continuous or repeated spoilage, negligence, errors in judgment, or similar instances that may cover subtle sabotage? Include an explanation of any such occurrences on record.

g. Are there any records of indications of disaffection? Explain and give details.

h. Is there an excessive amount of absenteeism among civilian employees? If so, what is the cause?

i. Is a record kept of monthly absenteeism? Spot check to determine if any individual is absent an excessive amount of time.

j. Is the monthly turnover excessive? If so, is it traceable to any reason or source of security significance? Explain.

D—31. Personnel Security, General

a. How many personnel are employed/assigned at the installation/activity? Give a breakdown of officers, enlisted men, and civilians.

b. What is the organization of the installation/activity? (Include a chart if applicable.)

c. How many foreign nationals are employed/assigned to the installation/activity?

(1) Do any foreign nationals engage in classified work or have access to classified information? How many?

(2) Indicate the date, degree of access, and approving authority of the authorization for access.

(3) Are any of the foreign nationals employed members of or in sympathy with subversive organizations or activities? If so, give details.

d. Have requirements of AR 604-20 been met for individuals engaged in information and education work? Spot check.

e. Have requirements of AR 50-3 been met for individuals with nuclear weapon responsibilities?

D—32. Communications System

a. What is the primary means of communications utilized on the installation?

b. What additional systems are used?

D—33. Security Measures

a. Does the installation have its own telephone system or does it use a commercial system? If it has its own system:

(1) Where are switchboards located?

(2) Are switchboards adequately guarded?

(3) Have switchboards been declared Restricted Areas?

(4) Are operators civilian or military?

(5) If civilian, how are they procured?

(6) Are operators cleared? To what degree?

(7) Are maintenance personnel civilian or military?

(8) If civilian, how are they procured?

(9) Are maintenance personnel cleared? To what degree?

(10) Are lines overhead or underground?

(11) Are open wires, terminal boxes, cross connecting boxes, cables, etc., protected and frequently inspected for indications of wiretapping? How?

(12) Is auxiliary power available in the event of a power failure? Explain.

(13) Are auxiliary parts available for repairs?

(14) What measures are taken to prevent discussion of classified information over the telephone?

b. Is there an approved circuit on the installation?

(1) Who was the approving authority?

(2) Describe the approved circuit.

(3) What parties are connected by the circuits?

(4) When and by whom is the circuit inspected for sabotage or tapping?

(5) What preventive measures are taken to secure the circuit?

c. If the installation uses a commercial telephone system:

(1) What company provides the service?

(2) What measures are taken to prevent dis-
cussion of classified information over the telephone?

(3) What measures are taken to prevent or detect wiretapping?

(4) When were previous CI technical surveys or inspections conducted?

d. Does the installation/activity have radio communications? If so:

(1) What type information is sent by radio? If classified, are code systems available? Has it been approved by USASA?

(2) Are the operators familiar with security requirements of radio transmissions?

e. Is teletype or telegraph used on the installation? If so:

(1) Where is it located?

(2) What security measures are taken to insure that classified information is not sent in the clear?

f. What measures are taken to insure that operators are adequately cleared?

g. When are inspections conducted by USASA?

h. Describe other communications media used on the installation. Include the safety precautions exercised to prevent unauthorized disclosure of classified information.

i. Does the installation/activity have a message center? If so:

(1) Where is the message center located?

(2) Give a detailed description of the message center, including measures taken to secure it from unauthorized access.

(3) Has the message center been declared a Restricted Area? Give details.

(4) Are message center personnel military or civilian? If civilian, where and how are they procured?

(5) Are the message center personnel cleared? To what degree? Is this sufficient for the category of information handled?

(6) Is someone on duty in the message center all times? Give details.

(7) What category of classified information is handled in the message center?

(8) What storage facilities are available?

(9) How is distribution made by the message center? Individual pickup, courier, delivery system?

j. Does the installation/activity utilize a courier service?

(1) Are the couriers military or civilian?

(2) Are the couriers cleared? To what degree?

(3) What category of classified material is carried by the couriers?

(4) Are couriers armed? With what weapon?

(5) What transportation is utilized by the couriers?

(6) Are couriers familiar with procedures to be followed in an emergency, such as an attempted or actual theft of classified material, vehicular accident, or other incident(s)?

k. What provisions for communications in the event of an emergency have been made? Describe in detail.

Section VI. UTILITIES

D-34. Electricity

a. What is the source of the electrical power for the installation/activity?

b. If purchased from a commercial source:

(1) Does power enter the installation through underground cable or overhead lines? Where do the lines enter the installation?

(2) What measures are taken to protect the power lines from tampering or sabotage?

(3) What is the peak load demand? Is the power received sufficient to provide an ample reserve beyond the peak load demand?

(4) Where is (are) the primary transformer station(s)? How are they protected?

(5) Where are substations? How are they protected?

(6) Who is responsible for maintenance of the power system?

(7) How frequently and by whom is the power system checked and inspected?

c. If power is generated on the installation:
(1) Where is (are) the powerhouse(s)?
(2) How are they protected from unauthorized access/sabotage?
(3) Is the amount of power generated sufficient to provide an ample reserve beyond the peak load demand?
(4) Where are the substations? How are they protected?
(5) Who is responsible for maintenance of the power system?
(6) When and by whom is the power system checked and inspected?
(7) Explain any other measures to protect the power system from sabotage.

d. What is the emergency power supply? Can it be actuated immediately?
(1) What activities are supplied with emergency power? Is the emergency source sufficient to provide the key facilities with electricity?
(2) Who is responsible for emergency power? Include maintenance and inspection.
(3) Is the emergency power source located in a secure area? Describe.

e. Is there a main blackout switch on the installation/activity? Who controls it? How is it protected? Where is it located?

D—35. Water
a. What is the source of water for the installation/activity?
   b. Is the source reasonably safe? Explain.
   c. If a public source is used, what is the diameter of the main and where does it enter the installation/activity?
   d. If a private system, reservoir, or tank is used, what is its capacity, water level, pressure, and condition? How is it secured?
   e. What is the water demand on the installation?
   f. Is the source adequate when compared to the demand?
   g. What is the water pressure on the mains?
   h. Are pumping stations protected? How? Where are they located?
   i. Are the pumps frequently inspected? When? By whom?
   j. Are mains, control valves, by-pass valves protected? How?
   k. How often is water tested for purification? By whom? How is the test made?
   l. Is an emergency water source available? Describe it to include location, capacity, potability.
   m. What type sewer system is used? Does it appear adequate for the needs of the installation/activity?

D—36. Heat
a. What is the source of heat for activities on the installation/activity?
   b. Is central heating provided? If so, where are the plants located and how are they protected?
   c. Is the heating system periodically inspected? When, by whom?
   d. Who is responsible for the heating system? Are maintenance personnel cleared if they are to have access to sensitive areas?
   e. Is there an emergency heating system? Describe it in detail.
   f. Where is fuel procured? Is it inspected to detect contamination? When, by whom? How is it stored? Where?
   g. If rooms are individually heated, what precautionary measures are taken to prevent fires?

Section VII. RECOMMENDATIONS

D—37. Recommendations
Careful consideration must be given to recommendations that are presented to the commander during the final briefing and when written in the Counterintelligence Survey Report. Recommendations must be feasible, realistic, and consistent with the overall sensitivity and importance of the installation or activity. Deficiencies in security should be concisely stated in pointing out what effect they may have on the command if allowed to continue, and solutions must be presented to correct them. Positive and concrete recommendations as opposed to suggestions should always be used.

D—38. Inspections
All items listed under Security of Information and Personnel Security may be used in a Counterintelligence Inspection.
APPENDIX E
NARCOTIC AND DRUG ABUSE GUIDE

E—1. General
Narcotic investigations should only be handled by Criminal Investigators of the USACIDC within the Army establishment except under exceptional circumstances which involve high level national security. Such instances should be coordinated at the highest practical level to determine if the case should continue under military intelligence jurisdiction, military police jurisdiction, or joint auspices.

E—2. Application
The most common instances when military intelligence Special Agents will require some knowledge of narcotics are:

a. Inductees who have qualified their DD Form 398 as pertaining to the use of narcotics.

b. When polygraph tracings indicate the use of a narcotic.

c. In routine or complaint type investigations where witnesses indicate the subject has used drugs and a subject interview becomes necessary.

d. When a human source has unexplained lapses of memory or other peculiar characteristics are demonstrated.

e. During the conduct of a special investigation involving unexplained affluence or indebtedness of a person in a sensitive or critical position requiring a security clearance.

E—3. Pharmacology of Drugs
Drugs are normally subdivided into four basic categories—depressants, stimulants, hallucinogens and narcotics—and each have general characteristics of their own within these basic groupings.

a. Stimulants. This group of drugs, which includes the amphetamines, directly stimulates the central nervous system, producing excitation, alertness, increased initiative and activity, and an ability to go without sleep for protracted periods of time. Amphetamines are prescribed for overweight patients, to reduce their appetites; in cases of narcolepsy, a disorder characterized by an overwhelming desire for sleep; for Parkinson's disease; and in some cases of minor mental depression. Because the body develops a tolerance to amphetamines, abusers increase their dosages gradually, which exaggerates the normal effects of these drugs and results in excitability, talkativeness, and can cause dryness of mouth, bad breath, tremor of the hands, enlarged pupils and heavy perspiration. Delusions and hallucinations can occur if used in a large quantity. In serious cases, a drug psychosis resembling schizophrenia develops with a psychic or emotional dependence on these drugs. Continued abuse of amphetamines can cause a person to exhibit dangerous, aggressive, antisocial behavior. Its physiological effects include high blood pressure, abnormal heart rhythms, and even heart attacks.

b. Depressants. This group includes the barbiturates, the most widely abused among the depressants. Barbiturates depress the central nervous system and are prescribed in small doses to relieve tension or to induce sleep. They are also valuable in cases of acute anxiety, hyperthyroidism, epilepsy, and high blood pressure. Because of their sedative but nonanalgesic effects, barbiturates are used in treating both physical and mental illnesses. Continued and excessive dosages of barbiturates result in slurring of speech, staggering, loss of balance and falling, quick temper, dilated pupils, and a quarrelsome disposition. Overdoses, particularly when taken in conjunction with alcohol result in unconsciousness and death, unless given proper medical treatment. While an unsteady gait and speech problems may be signs of neurological disorders, such as multiple sclerosis, such diseases are uncommon among young men. Usually, the appearance of drunkenness without an alcoholic breath indicates barbiturate intoxication but it must also be noted that many diseases will manifest such an appearance; therefore, this should only be used as an indicator. Although physical dependence does not develop
with the dosages normally used in medical practice, it does occur with the excessive doses used by drug abusers. A tolerance is also developed. Withdrawal symptoms usually are far more dangerous than those resulting from narcotics withdrawal. In addition to the strictly depressant drugs, another group of drugs, tranquilizers, particularly those in the phenothiazine derivative group, are frequently sought after and abused. While they will not cause sleep except in high dosages, and are not purely depressive or stimulatory, they will impair an individual's judgment even to the point of complete disregard for any applicable security requirements.

c. Hallucinogens. This group consists of the so-called psychotomimetic agents, and are so named because they may produce hallucinations or illusions of the various senses. When experiencing an hallucination or illusion, a person's ability to perceive is based not upon objective reality but upon distortion or imagination. Most of the hallucinogenic drugs, such as lysergic acid diethylamide (LSD), in illicit channels of distribution are manufactured in clandestine laboratories. Legitimate chemical manufacturers do produce some of the hallucinogenic drugs, but only for investigational purposes. Some of these drugs have been diverted to the illicit market through thefts of illegal purchases. Although openly and irresponsibly promoted as a means of expanding consciousness, the hallucinogens have yet to be proven valuable medically. Hence, there are neither standard dosage forms nor markings which make visual identification possible. Illicit laboratories produce hallucinogens in the form of capsules, tablets, powders, or liquids, which peddlers and users often disguise in common personal items, such as sugar cubes, candy, paper, aspirin, jewelry, liquor, cloth, or even postage stamps. Usually hallucinogens distort or intensify the user's sense perceptions and lessen his ability to discriminate between fact and fantasy. A user may speak of “seeing” sound and “hearing” colors. He will appear to be in a trance-like state, and will have an increase in heart rate, blood sugar and blood pressure. His pupils are dilated and sensitive to light. Perceptual changes in all senses may occur, and he may become fearful and experience terror. Restlessness and sleeplessness are common until the drug wears off. The user can have nausea, chills, flushing, irregular breathing, sweating and trembling hands. Mental effects of the drugs are unpredictable and include illusions, exhilaration, withdrawal from society, ideas of violence or self-destruction, or sheer panic. This variability of hallucinogenic drug effect is a definite danger to users. The spontaneous occurrence of “flash backs” of prior hallucinations is another harmful effect of certain hallucinogens, particularly LSD.

d. Narcotics. This group of drugs consists of opium, coca leaves, as well as any preparation, salts and compounds of these, and synthetics derived from these basic drugs. Narcotics are used medically to relieve pain and produce sleep or drowsiness. Heroin and codeine, both of which are derivatives of opium, are the most common drugs in this category. Heroin is found in varying shades from snow white to light brown, is odorless, and has a bitter taste; however, suspicious white powders should not be tasted by any Special Agent as a check on the narcotic. Heroin is usually taken intravenously (mainlined) but it can also be taken orally or by inhalation. An addict or user who mainlines normally will have in his possession, or accessible, the “paraphernalia” necessary for mainlining. This normally includes a spoon with a bent handle, matches, medicine dropper, hypodermic needle, and maybe a rubber tube which he will use as a tourniquet to make his vein stand out for easier injections. Dosage can begin as small as 2mg a day and work up to 450mg a day. The mere possession of paraphernalia will give civilian police and CIDC “probable cause” to detain the suspect. An addict or user on heroin can manifest the following symptoms: lethargy, drowsiness, constricted pupils, itchiness, constipation, upset stomach, watering eyes, runny nose. With hard narcotics, there are four factors which will cause addiction. These factors are:

(1) Compulsion—desire for the drug.
(2) Tolerance—the increasing limits of consumption.
(3) Physical—the craving for the drug which will result in withdrawals when taken away.
(4) Psychological—the belief that the drug is necessary.

E-4. Indicators

a. Since drugs are found in common usage in solid, powder, and liquid forms, and taken in various forms, an investigation of a purely drug use case should be performed by qualified personnel from the local CIDC office. The CIDC has automatic jurisdiction over drug use, which is a criminal offense, unless security matters override, which should be rare. Indications are that be-
cause of the control problems presented by an addict or user, hostile intelligence services will not recruit a user except on a one-time job. However, to determine if a person might be a security threat as a result of drug use, the following indicators are given:

1. The physical characteristics as described under each category above.
2. When a person hides pills or liquids which appear to be legitimate.
3. Old prescription bottles are suspect.
4. A name different from the suspect's on a prescription bottle.
5. Strong odors emulating from cigarettes.
6. “Tracks" or tattoo appearing scars on the arms, wrists, feet or hands which could be a result of mainlining.
7. A redness or swelling in the partition of the nose.
8. A sallow complexion, trembling hands, dilated eyes, going on the nod or sleeplessness.
9. Long periods of time in the latrine at regular intervals, such as every 4 or 8 hours.
10. Wearing of sunglasses.
11. Sloppy appearance.
12. Uncontrollable temper.
13. Long shirt sleeves on hot days.
15. Unexplained affluency.
16. Theft.
17. Constant borrowing of money from co-workers.
18. Inattention to dress or personal hygiene.
19. Association with drug users.
20. Personality changes.
21. Gaiety followed by marked depression.
22. Cold skin.
23. Possession of blank or undated prescription forms.

b. It must be remembered at all times that some individuals have a legitimate need and use for drugs such as a diabetic, or an individual with thyroid problems. Any suspicious activity on the part of an employee or soldier where doubt still remains should not be investigated by military intelligence but by the CIDC.

E-5. Detection
Drugs in the usual dosages taken by addicts will remain within the individual's system for about 8 to 10 hours and may be detected by various tests. One of the tests is a urinalysis. However, in addition, there are field test kits which can be purchased for testing of a suspicious liquid or substance, but these kits will not prove the existence of a particular drug. They will only indicate the possibility of its existence. Also, the average life expectancy of some kits is only 30 to 90 days. Other drugs, like LSD, will fluoresce when subjected to ultraviolet light. Special training is needed before becoming qualified to depend on the various tests as accurate indicators for detection of drugs in the body.

E-6. Marihuana
Marihuana and cocaine are both classed as narcotics from a law enforcement standpoint and will impose a psychological dependence on the abuser, but marihuana is a hallucinogen while cocaine is a stimulant for all practical purposes. Neither are known to cause physical dependence or develop a tolerance; however, both are dangerous if abused. Marihuana can cause hallucinations similar to LSD, and can produce symptoms such as distortion of depth and time perception. While under the drug, the eyes may become pink. Abusers are difficult to identify unless under the influence of the drug. Under the influence, they may appear animated and hysterical which may be expressed by loud talk and laughter. Marihuana will cause a loss of coordination, distortion of visual and auditory sensations, impairment of judgment and memory, confusion and delusions. Hashish is a concentrated marihuana which has been created by obtaining the resin from the growing plant or a similar method. Marihuana the drug is obtained from the plant Cannabis sativa L., and consists of the leaves, flowers, stems, and seeds but not the stalk. Marihuana plants are bisexual, and can be positively identified under a microscope since it is profusely covered with fine hair, but better identification can be made from the leaves, seeds, and seed hull even if the plant has been finely crushed. The most distinctive identification is the cystolith hair on the upper side of the leaflet consisting of a stactic and a gradular hair. Visually, identification can be made by inspecting the plant. Basically, the leaves are compound, and normally consist of from five to eleven leaflets with seven an average. The stalk will grow from 3 to 16 feet in height with an average height of 4 to 6 feet. The leaves are jagged in appearance.
<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>“ABC” method of surveillance (fig 4-1)</td>
<td>4-27b, 4-18</td>
</tr>
<tr>
<td>“AB” method of surveillance (fig 4-2)</td>
<td>4-27b, 4-18</td>
</tr>
<tr>
<td>Accreditation of special agent</td>
<td>1-2, 1-1</td>
</tr>
<tr>
<td>Accused person, Rights of</td>
<td>3-6, 3-2</td>
</tr>
<tr>
<td>Administrative oaths</td>
<td>3-27, 3-11</td>
</tr>
<tr>
<td>Administrative proceedings</td>
<td>3-2b, 3-4, 3-1, 3-2, 3-6b, 4-3e, 4-2</td>
</tr>
<tr>
<td>Admissions</td>
<td>3-6, 5-12, 3-2, 5-8</td>
</tr>
<tr>
<td>Adverse information</td>
<td>8-19, 8-5</td>
</tr>
<tr>
<td>Advising of rights</td>
<td>3-6, 3-16, 3-2, 3-9, 4-12, 4-8, 5-20d, 5-10</td>
</tr>
<tr>
<td>Advocating overthrow of US Government</td>
<td>9-19, 9-7</td>
</tr>
<tr>
<td>Affidavit</td>
<td>app B, B-1</td>
</tr>
<tr>
<td>Agent: Notes</td>
<td>app B, B-1</td>
</tr>
<tr>
<td>Report</td>
<td>7-5, app B, 7-2, B-1</td>
</tr>
<tr>
<td>Special</td>
<td>1-2</td>
</tr>
<tr>
<td>Agreement: Delimitations</td>
<td>1-4a, 1-2</td>
</tr>
<tr>
<td>Status of forces</td>
<td>1-4c, 1-2</td>
</tr>
<tr>
<td>Aiding the enemy</td>
<td>9-15, 9-6</td>
</tr>
<tr>
<td>Air reconnaissance and surveillance</td>
<td>2-9d, 2-5</td>
</tr>
<tr>
<td>Allied forces</td>
<td>6-15c, 6-4</td>
</tr>
<tr>
<td>Amphetamines</td>
<td>app E, E-1</td>
</tr>
<tr>
<td>Announced counterintelligence inspections</td>
<td>10-16a, 10-8</td>
</tr>
<tr>
<td>Apprehension</td>
<td>3-8, 3-14, 3-7, 3-8, 4-17d, 4-13</td>
</tr>
<tr>
<td>Approach: To elicitation</td>
<td>4-21, 4-14</td>
</tr>
<tr>
<td>To interviews</td>
<td>4-9, 4-6</td>
</tr>
<tr>
<td>Area: Army, organization</td>
<td>2-4, 2-1</td>
</tr>
<tr>
<td>Coverage</td>
<td>12-5a, 13-9, 12-3, 13-5</td>
</tr>
<tr>
<td>Rear</td>
<td>2-7, 2-3</td>
</tr>
<tr>
<td>Area support: Command</td>
<td>2-8, 2-4</td>
</tr>
<tr>
<td>Group</td>
<td>2-8a, 2-4</td>
</tr>
<tr>
<td>MI Company (CI) (fig 2-6)</td>
<td>2-12, 2-7</td>
</tr>
<tr>
<td>MI Detachment (CRF) (fig 2-5)</td>
<td>2-10, 2-5</td>
</tr>
<tr>
<td>MI Group (CI) (fig 2-3)</td>
<td>2-8, 2-4</td>
</tr>
<tr>
<td>MI Group (CI) (fig 2-3, 2-4)</td>
<td>2-8</td>
</tr>
<tr>
<td>Army: Area organization</td>
<td>2-4, 2-1</td>
</tr>
<tr>
<td>Field</td>
<td>2-7b, 2-4</td>
</tr>
<tr>
<td>Security Agency</td>
<td>4-32b, 4-27, 10-1d, 10-1, 10-12d, 10-7</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theater</td>
<td>11-2, 11-1, 12-11e, 12-8</td>
</tr>
<tr>
<td>Arrest, authority</td>
<td>2-7a, 2-3</td>
</tr>
<tr>
<td>ASCOM (area support command): MI Company (CI) (fig 2-6)</td>
<td>2-12, 2-7</td>
</tr>
<tr>
<td>MI Detachment (CRF) (fig 2-5)</td>
<td>2-10, 2-5</td>
</tr>
<tr>
<td>MI Group (CI) (fig 2-3)</td>
<td>2-8, 2-4</td>
</tr>
<tr>
<td>HQ MI Group (CI) (fig 2-4)</td>
<td>2-9, 2-4</td>
</tr>
<tr>
<td>Audio surveillance (fig 5-1, 5-2)</td>
<td>5-2a, 5-3, 5-1, 5-2</td>
</tr>
<tr>
<td>Equipment</td>
<td>5-4, 11-2, 5-2, 11-1</td>
</tr>
<tr>
<td>Augmentation: Civil police</td>
<td>12-10a, 12-6</td>
</tr>
<tr>
<td>Tactical troops</td>
<td>12-10a, 12-6</td>
</tr>
<tr>
<td>Background Investigations: Components</td>
<td>8-4, 8-1</td>
</tr>
<tr>
<td>Scope</td>
<td>8-3, 8-1</td>
</tr>
<tr>
<td>Bad credit</td>
<td>8-16, 8-4</td>
</tr>
<tr>
<td>Barbiturates</td>
<td>app E, E-1</td>
</tr>
<tr>
<td>Blacklist</td>
<td>12-9a, 12-5, 12-11b, 12-8</td>
</tr>
<tr>
<td>Block control</td>
<td>13-6h, 13-5</td>
</tr>
<tr>
<td>Border: Control</td>
<td>13-6, 13-3</td>
</tr>
<tr>
<td>Security</td>
<td>12-16h, 12-16, 14-11f, 14-4</td>
</tr>
<tr>
<td>Base camp security</td>
<td>13-10, 13-5</td>
</tr>
<tr>
<td>“Bugging”</td>
<td>5-5, 5-4</td>
</tr>
<tr>
<td>Casual source</td>
<td>6-4b, 6-2</td>
</tr>
<tr>
<td>Central Intelligence Agency (CIA)</td>
<td>8-15b, 8-4</td>
</tr>
<tr>
<td>Central records facility (fig 2-5)</td>
<td>2-10, 2-5</td>
</tr>
<tr>
<td>Characterization</td>
<td>7-8, 7-3</td>
</tr>
<tr>
<td>Individual</td>
<td>app B, B-1</td>
</tr>
<tr>
<td>Organization</td>
<td>app B, B-1</td>
</tr>
<tr>
<td>Checklist</td>
<td>10-4, 11-4, 11-2, app D, D-1</td>
</tr>
<tr>
<td>Checkpoint</td>
<td>4-27c, 4-22</td>
</tr>
<tr>
<td>Mobile</td>
<td>12-16h, 12-16, 14-11f, 14-4</td>
</tr>
<tr>
<td>Surveillance</td>
<td>4-27c, 4-22</td>
</tr>
<tr>
<td>Static (fig 12-2)</td>
<td>12-16h, 12-16, 14-11f, 14-4</td>
</tr>
<tr>
<td>Circulation control</td>
<td>14-11g, 14-4</td>
</tr>
<tr>
<td>Citizenship</td>
<td>8-13, 8-4</td>
</tr>
<tr>
<td>Civil affairs</td>
<td>2-7, 2-9, 2-3, 2-4, 12-9, 12-5, 12-12a, 12-10, 12-16, 12-12, 14-1, 14-2, 14-3, 14-8</td>
</tr>
</tbody>
</table>

Index-1
<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Civil disturbances</td>
<td>12-12b, 12-12d</td>
</tr>
<tr>
<td>Civil police, augmentation</td>
<td>12-10a</td>
</tr>
<tr>
<td>Civil security</td>
<td>12-3b, 14-2</td>
</tr>
<tr>
<td>Clandestine listening devices</td>
<td>11-7</td>
</tr>
<tr>
<td>Clearances, indigenous labor force</td>
<td>2-9a</td>
</tr>
<tr>
<td>Close surveillance</td>
<td>4-25a</td>
</tr>
<tr>
<td>Cocaine app E</td>
<td></td>
</tr>
<tr>
<td>Codes 4-26f, 4-32b</td>
<td></td>
</tr>
<tr>
<td>Collection of physical evidence</td>
<td>4-31</td>
</tr>
<tr>
<td>Combat counterintelligence</td>
<td>12-11</td>
</tr>
<tr>
<td>Combination surveillance</td>
<td>4-25b, 4-27e</td>
</tr>
<tr>
<td>Communications</td>
<td>4-26f, 4-27f</td>
</tr>
<tr>
<td>Communications security</td>
<td>10-1d</td>
</tr>
<tr>
<td>Complaint investigation: Categories</td>
<td>9-3</td>
</tr>
<tr>
<td>Conduct</td>
<td>9-7, 9-10, 9-2, 9-4, 9-9, 9-12, 9-16, 9-6, 9-21, 9-7</td>
</tr>
<tr>
<td>Incident</td>
<td>9-2a</td>
</tr>
<tr>
<td>Personal</td>
<td>9-2b</td>
</tr>
<tr>
<td>Components of a Background Investigation</td>
<td>8-4</td>
</tr>
<tr>
<td>Compromise of surveillance</td>
<td>4-28b</td>
</tr>
<tr>
<td>Confessions</td>
<td>3-16, 3-14, 3-2, 3-8, 3-9, 4-5, 4-17, 4-14, 5-12</td>
</tr>
<tr>
<td>Confidential source</td>
<td>6-5</td>
</tr>
<tr>
<td>Consent search (fig 3-1)</td>
<td>3-7b</td>
</tr>
<tr>
<td>Consolidation operations</td>
<td>14-14a</td>
</tr>
<tr>
<td>Conspiracy, sedition</td>
<td>9-18</td>
</tr>
<tr>
<td>CONUS (Continental United States)</td>
<td></td>
</tr>
<tr>
<td>Military Intelligence group (fig 2-2)</td>
<td>2-4</td>
</tr>
<tr>
<td>National agencies</td>
<td>6-13</td>
</tr>
<tr>
<td>Special counterintelligence units</td>
<td>2-6</td>
</tr>
<tr>
<td>Tactical counterintelligence elements</td>
<td>2-5</td>
</tr>
<tr>
<td>Conventional source</td>
<td>6-4, app B 6-1, B-1</td>
</tr>
<tr>
<td>Conversation</td>
<td>4-22</td>
</tr>
<tr>
<td>&quot;Convoy&quot;</td>
<td>4-29a</td>
</tr>
<tr>
<td>Cordon and search operations (fig 13-1, 13-2, 13-3)</td>
<td>13-10b</td>
</tr>
<tr>
<td>Assistance from PSYOP</td>
<td>14-14a</td>
</tr>
<tr>
<td>With military police</td>
<td>14-11k</td>
</tr>
<tr>
<td>Counsel, refusal of</td>
<td>3-6d</td>
</tr>
<tr>
<td>Counterspy</td>
<td>9-12</td>
</tr>
<tr>
<td>Investigations</td>
<td>9-10</td>
</tr>
<tr>
<td>Counterterrorism: Area coverage</td>
<td>12-5a, 13-8</td>
</tr>
<tr>
<td>Augmentation</td>
<td>12-10</td>
</tr>
<tr>
<td>Employment</td>
<td>1-2, 2-3</td>
</tr>
<tr>
<td>Indications</td>
<td>12-11e, 12-8, 12-16</td>
</tr>
<tr>
<td>Inspection</td>
<td>10-14</td>
</tr>
<tr>
<td>Interrogations</td>
<td>3-6a, 12-11</td>
</tr>
<tr>
<td>Interviews</td>
<td>4-7, 4-10, 4-5, 4-6, 4-12, 4-8</td>
</tr>
<tr>
<td>Investigations</td>
<td>12-3e, 4-1, 4-16, 4-12, 12-12a</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>1-3</td>
</tr>
<tr>
<td>Limitations</td>
<td>1-4</td>
</tr>
<tr>
<td>Mission</td>
<td>1-3</td>
</tr>
<tr>
<td>Offensive</td>
<td>1-5a</td>
</tr>
<tr>
<td>Officer</td>
<td>1-2</td>
</tr>
<tr>
<td>Organization</td>
<td>2-2</td>
</tr>
<tr>
<td>Principles</td>
<td>1-5</td>
</tr>
<tr>
<td>Personnel</td>
<td>1-2</td>
</tr>
<tr>
<td>Services</td>
<td>1-3b</td>
</tr>
<tr>
<td>Special operations</td>
<td>1-3c</td>
</tr>
<tr>
<td>Spot reports</td>
<td>7-11</td>
</tr>
<tr>
<td>Stability operations</td>
<td>13-1</td>
</tr>
<tr>
<td>Survey</td>
<td>10-1, 10-1</td>
</tr>
<tr>
<td>Tactical operations</td>
<td>12-3, 12-6, 12-1, 12-4</td>
</tr>
<tr>
<td>Technical inspection</td>
<td>11-1b, 11-2d, 11-1, 11-3e</td>
</tr>
<tr>
<td>Technical surveys</td>
<td>11-1e, 11-1, 11-2, 11-3a</td>
</tr>
<tr>
<td>Countersabotage</td>
<td>9-7</td>
</tr>
<tr>
<td>Countersubversion</td>
<td>9-23</td>
</tr>
<tr>
<td>Credit, bad</td>
<td>8-16</td>
</tr>
<tr>
<td>Crime: Definition</td>
<td>3-3</td>
</tr>
<tr>
<td>Prevention surveys</td>
<td>10-3, 10-3, 10-6, D-1</td>
</tr>
<tr>
<td>Criminal Investigation Command, US Army</td>
<td>6-15e, 6-4, 10-3, 10-6, app E</td>
</tr>
<tr>
<td>Depressant</td>
<td>5-15a, 5-9, E-1</td>
</tr>
<tr>
<td>Derogatory information: Loyalty</td>
<td>8-19b</td>
</tr>
<tr>
<td>Suitability</td>
<td>8-19a</td>
</tr>
<tr>
<td>Rebutted</td>
<td>3-18a</td>
</tr>
<tr>
<td>Detecting surveillance</td>
<td>4-29</td>
</tr>
<tr>
<td>Detection equipment</td>
<td>11-5</td>
</tr>
<tr>
<td>Directives, National Security</td>
<td>1-4b</td>
</tr>
<tr>
<td>Disaffection</td>
<td>9-24</td>
</tr>
<tr>
<td>Disclosure of official information</td>
<td>4-11g</td>
</tr>
<tr>
<td>Discreet surveillance</td>
<td>4-25a</td>
</tr>
<tr>
<td>Document: Security</td>
<td>10-10</td>
</tr>
<tr>
<td>Transfer</td>
<td>12-4a</td>
</tr>
<tr>
<td>Documentary: Evidence</td>
<td>4-32</td>
</tr>
<tr>
<td>Source</td>
<td>6-6</td>
</tr>
</tbody>
</table>

Index-2
<table>
<thead>
<tr>
<th>Obtained from Government Agencies</th>
<th>6-15b, 6-4, app B B-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Official disclosure of</td>
<td>4-11g 4-7</td>
</tr>
<tr>
<td>Security of</td>
<td>10-10, 10-5, 13-4 13-2</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>14-4c 14-1</td>
</tr>
<tr>
<td>Inspection:</td>
<td></td>
</tr>
<tr>
<td>Announced</td>
<td>10-16a 10-8</td>
</tr>
<tr>
<td>Counterintelligence</td>
<td>10-14 10-7</td>
</tr>
<tr>
<td>Penetration</td>
<td>10-16c 10-8</td>
</tr>
<tr>
<td>Reports</td>
<td>10-17, 10-9, 11-8, 11-3, app C C-1</td>
</tr>
<tr>
<td>Technical</td>
<td>11-15, 11-1, 11-2, 11-3, 11-5b 10-16b 10-8</td>
</tr>
<tr>
<td>Unannounced</td>
<td></td>
</tr>
<tr>
<td>Installation:</td>
<td></td>
</tr>
<tr>
<td>Target</td>
<td>12-9 12-5</td>
</tr>
<tr>
<td>Sensitivity</td>
<td>10-8 10-4</td>
</tr>
<tr>
<td>Security</td>
<td>13-10 13-5</td>
</tr>
<tr>
<td>Intelligence:</td>
<td></td>
</tr>
<tr>
<td>Agencies</td>
<td>6-13, 6-15 6-4</td>
</tr>
<tr>
<td>Command (fig 2-1)</td>
<td>2-4, 2-9c 2-1, 2-5, 11-5 11-2</td>
</tr>
<tr>
<td>Technical</td>
<td>6-11, 6-3, 14-15 14-4</td>
</tr>
<tr>
<td>Collection potential of Civil Affairs</td>
<td>14-8 14-3</td>
</tr>
<tr>
<td>Police, reciprocal</td>
<td>14-11a, 14-12 14-3, 14-4</td>
</tr>
<tr>
<td>Interpreters</td>
<td>3-24, 3-11, 4-89, 4-32, 5-18, 5-10, 12-12a, 12-10, 13-11 13-9</td>
</tr>
<tr>
<td>Interrogation</td>
<td>4-16 4-12</td>
</tr>
<tr>
<td>Accused and suspects</td>
<td>3-6, 4-17, 3-2, 4-12, 5-12, 5-8, 9-7b 9-2</td>
</tr>
<tr>
<td>Combat</td>
<td>12-11 12-7</td>
</tr>
<tr>
<td>Conduct of</td>
<td>4-17e 4-14</td>
</tr>
<tr>
<td>Detailed</td>
<td>12-11g 12-10</td>
</tr>
<tr>
<td>Preparation for</td>
<td>4-17d 4-13</td>
</tr>
<tr>
<td>Screening</td>
<td>12-11f 12-9</td>
</tr>
<tr>
<td>Halting of</td>
<td>3-6g 3-4</td>
</tr>
<tr>
<td>Interviews</td>
<td>4-7, 4-10 4-5, 4-6</td>
</tr>
<tr>
<td>Approach</td>
<td>4-9 4-6</td>
</tr>
<tr>
<td>Attempts</td>
<td>app B B-1</td>
</tr>
<tr>
<td>Females</td>
<td>4-12d 4-8</td>
</tr>
<tr>
<td>Preparation for</td>
<td>4-8 4-5</td>
</tr>
<tr>
<td>Rapport</td>
<td>4-9g 4-6</td>
</tr>
<tr>
<td>Subject</td>
<td>4-12 4-8</td>
</tr>
<tr>
<td>&quot;Walk-ins&quot;</td>
<td>4-13 4-9</td>
</tr>
<tr>
<td>Witness</td>
<td>4-14 4-10</td>
</tr>
<tr>
<td>Illiterates</td>
<td>4-40 4-32</td>
</tr>
<tr>
<td>Investigation:</td>
<td></td>
</tr>
<tr>
<td>Background</td>
<td>8-2 8-1</td>
</tr>
<tr>
<td>Complaint</td>
<td>9-1, app E E-1</td>
</tr>
<tr>
<td>Counterespionage</td>
<td>9-10, 9-12 9-4</td>
</tr>
<tr>
<td>Counterintelligence</td>
<td>4-1 4-1</td>
</tr>
<tr>
<td>Countersabotage</td>
<td>9-7 9-2</td>
</tr>
<tr>
<td>Countersubversion</td>
<td>9-23 9-8</td>
</tr>
<tr>
<td>Disaffection</td>
<td>9-24 9-8</td>
</tr>
<tr>
<td>Indigenous persons</td>
<td>12-12a, 12-10, 14-4 14-1</td>
</tr>
<tr>
<td>Limitations of</td>
<td>1-4 1-2</td>
</tr>
<tr>
<td>Mutiny</td>
<td>9-20a 9-7</td>
</tr>
<tr>
<td>National Agency Check</td>
<td>8-2, 8-5 8-1, 8-2</td>
</tr>
<tr>
<td>Personnel Security</td>
<td>8-1, 13-3, 13-2, app E E-1</td>
</tr>
<tr>
<td>Riots and civil disturbances</td>
<td>12-12b 12-11</td>
</tr>
<tr>
<td>Security</td>
<td>1-3a 1-1</td>
</tr>
<tr>
<td>Seditious conspiracy</td>
<td>9-18, 9-7</td>
</tr>
<tr>
<td>Treason</td>
<td>9-16 9-6</td>
</tr>
<tr>
<td>Investigative:</td>
<td></td>
</tr>
<tr>
<td>Agencies</td>
<td>6-15 6-4</td>
</tr>
<tr>
<td>Guides</td>
<td>9-10 9-4</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>1-6d, 1-3, 13-9 13-5</td>
</tr>
<tr>
<td>Legal principles</td>
<td>3-1 3-1</td>
</tr>
<tr>
<td>Photography</td>
<td>5-2c, 5-7 5-1, 5-5</td>
</tr>
<tr>
<td>Plan</td>
<td>4-2 4-1</td>
</tr>
<tr>
<td>Procedures</td>
<td>9-7, 9-12, 9-2, 9-4, 9-16, 9-6, 9-21 9-7</td>
</tr>
<tr>
<td>Judge Advocate General (JAG)</td>
<td>3-4b, 3-6 3-2</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>1-3, 13-2, 1-1, 13-1, 13-9 13-5</td>
</tr>
<tr>
<td>Key Sheet (fig B-7)</td>
<td>app B B-1</td>
</tr>
<tr>
<td>Lawfully obtained evidence</td>
<td>3-2b, 5-2c 3-1, 5-1 4-11i, 4-7, app B B-1</td>
</tr>
<tr>
<td>Lead</td>
<td></td>
</tr>
<tr>
<td>From Government agencies</td>
<td>6-15b, 6-4, app B B-1</td>
</tr>
<tr>
<td>From records</td>
<td>4-8a 4-1</td>
</tr>
<tr>
<td>Jurisdictional</td>
<td>app B B-1</td>
</tr>
<tr>
<td>Sheet</td>
<td>app B B-1</td>
</tr>
<tr>
<td>Subsidiary</td>
<td>app B B-1</td>
</tr>
<tr>
<td>&quot;Throw Offs&quot;</td>
<td>app B B-1</td>
</tr>
<tr>
<td>Legal principles</td>
<td>3-1</td>
</tr>
<tr>
<td>Liaison</td>
<td>4-6b, 4-5, 6-12 6-3</td>
</tr>
<tr>
<td>Allied forces</td>
<td>6-15c, 6-4, 14-1 14-1</td>
</tr>
<tr>
<td>Civil affairs</td>
<td>14-1, 14-2 14-1</td>
</tr>
<tr>
<td>CONUS agencies</td>
<td>6-15, 6-14</td>
</tr>
<tr>
<td>Host country</td>
<td>6-15e 6-4</td>
</tr>
<tr>
<td>Imagery interpretation</td>
<td>14-15 14-4</td>
</tr>
<tr>
<td>Military police</td>
<td>14-1, 14-1, 14-10, 14-3</td>
</tr>
<tr>
<td>Order of battle</td>
<td>14-15 14-4</td>
</tr>
<tr>
<td>Overseas agencies</td>
<td>6-15 6-4</td>
</tr>
<tr>
<td>Psychological warfare</td>
<td>14-1, 14-3 14-1</td>
</tr>
<tr>
<td>Signal intelligence</td>
<td>14-15 14-4</td>
</tr>
<tr>
<td>Technical intelligence</td>
<td>14-15 14-4</td>
</tr>
<tr>
<td>&quot;Third agency rule&quot;</td>
<td>6-15b 6-4</td>
</tr>
<tr>
<td>Limitations, Counterintelligence</td>
<td>1-4 1-2</td>
</tr>
<tr>
<td>Local agency check</td>
<td>8-11 8-3</td>
</tr>
</tbody>
</table>

Index-4
<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principles</td>
<td>2-2</td>
</tr>
<tr>
<td>Special elements</td>
<td>2-6</td>
</tr>
<tr>
<td>Target</td>
<td>12-9</td>
</tr>
<tr>
<td>Theater Army</td>
<td>2-7a</td>
</tr>
<tr>
<td>US Army Intelligence Command (fig 2-1)</td>
<td>2-4</td>
</tr>
<tr>
<td>Pattern: Analysis</td>
<td>13-12</td>
</tr>
<tr>
<td>Behavioral</td>
<td>12-5b</td>
</tr>
<tr>
<td>Penetration inspections</td>
<td>10-16e</td>
</tr>
<tr>
<td>Personnel: Complaint investigation</td>
<td>9-2b</td>
</tr>
<tr>
<td>Document source</td>
<td>6-9</td>
</tr>
<tr>
<td>Personnel: Blacklist</td>
<td>12-9a</td>
</tr>
<tr>
<td>Counterintelligence</td>
<td>1-2</td>
</tr>
<tr>
<td>Gray list</td>
<td>12-9a</td>
</tr>
<tr>
<td>Indigenous</td>
<td>12-12a</td>
</tr>
<tr>
<td>Security Investigation</td>
<td>4-1, 8-1</td>
</tr>
<tr>
<td>Selection for surveillance target</td>
<td>4-26a</td>
</tr>
<tr>
<td>White list</td>
<td>12-8a</td>
</tr>
<tr>
<td>Personnel Security Investigations (PSI)</td>
<td>8-1</td>
</tr>
<tr>
<td>Components of</td>
<td>8-4</td>
</tr>
<tr>
<td>In stability operations</td>
<td>13-3</td>
</tr>
<tr>
<td>Indigenous personnel</td>
<td>12-12a</td>
</tr>
<tr>
<td>Request for</td>
<td>app B</td>
</tr>
<tr>
<td>Scope</td>
<td>B-1</td>
</tr>
<tr>
<td>Sworn Statements in</td>
<td>B-1</td>
</tr>
<tr>
<td>Photography, investigative (fig 5-3)</td>
<td>5-2, 5-7</td>
</tr>
<tr>
<td>Physical evidence (fig 4-4)</td>
<td>4-31</td>
</tr>
<tr>
<td>Physical security</td>
<td>10-12</td>
</tr>
<tr>
<td>Planning: Investigation</td>
<td>4-2</td>
</tr>
<tr>
<td>Tactical operations</td>
<td>12-7, 13-1</td>
</tr>
<tr>
<td>Political apparatus study</td>
<td>13-1c</td>
</tr>
<tr>
<td>Polygraph</td>
<td>4-18</td>
</tr>
<tr>
<td>Populace control</td>
<td>13-6</td>
</tr>
<tr>
<td>Port security</td>
<td>12-16d</td>
</tr>
<tr>
<td>Private document source</td>
<td>6-9</td>
</tr>
<tr>
<td>Priority target</td>
<td>12-8</td>
</tr>
<tr>
<td>Progressive surveillance</td>
<td>4-27d</td>
</tr>
<tr>
<td>Propaganda: Black</td>
<td>14-14f</td>
</tr>
<tr>
<td>Grey</td>
<td>14-14f</td>
</tr>
<tr>
<td>Subversive</td>
<td>14-14g</td>
</tr>
<tr>
<td>Protection of: Of investigative reports</td>
<td>7-4, 11-3</td>
</tr>
<tr>
<td>Of sources</td>
<td>6-4, 6-5</td>
</tr>
</tbody>
</table>

**Lysergic acid diethylamide (LSD)**

**Marijuana**

**Material sources** 6-10

**Material targets** 12-9

**Media analysis** 14-14d

**Military Intelligence Battalion** 2-9

**Military Intelligence Group:**

CONUS (fig 2-2) 2-4

ASCOM (fig 2-3) 2-3

**Military Police** 2-9a, 2-4, 10-4a, 10-2, 10-12, 10-7, 13-10, 13-5, 14-1, 14-1, 14-10, 14-3, 14-11, app C, C-1, app D, D-1, app E E-l

**Mission, Counterintelligence** 1-3

**Misuse of Counterintelligence personnel** 5-6a 5-5

**Mixed surveillance** 4-27b, 4-16, 4-27c 4-22

**Moving surveillance** 4-27b 4-18

**Mutiny** 9-20a 9-7

**Narcotics** 5-15d, 5-9, app E E-1

**National Agency Check** 8-2, 8-5 8-1, 8-5

**National Security Check** 7-10 7-3

**National Security Directives** 1-4b 1-2

**Naval Investigative Service** 1-4a 1-2

**Negative information** 4-4e 4-2

**Notes:**

Agent app B B-1

Taking 4-11 4-7, 4-13b 4-9

Oaths, administration of 3-25, 3-27 3-11

**Offensive counterespionage** 1-5e 1-3

**Office of Special Investigation (OSI)** 1-4 1-2

**Officer, Counterintelligence** 1-2 1-1

**Official sources** 6-4e, 6-2, 6-15c 6-4

**One vehicle/man method of surveillance (fig 4-3)** 4-27b 4-18

**Operations:**

**Defensive:** 1-5e 1-3

**Offensive** 1-5e 1-3

**Other** 12-6 12-4

**Screening** 12-16 12-12

**Special** 1-8c 1-2

**Stability** 18-1 13-1

**Tactical** 12-4, 12-2, 12-5, 12-3, 12-15 12-12

**Order of Battle liaison** 14-15

**Organization:**

ASCOM 2-8

CONUS 2-4, 2-5 2-1, 2-2

Field Army 2-7b 2-4

**Physical evidence (fig 4-4)** 4-31 4-27

**Physical security** 10-12, 10-7, 11-3, 11-2, 12-16d, 12-16, 13-5, 13-5, 14-11a, 14-4, app D D-1

**Photography, investigative (fig 5-3)** 5-2, 5-7, 5-1, 5-5, 5-8 5-7

**Polygraph** 4-18, 4-14, 5-2e 5-2, 5-12, 5-8, app E E-1

**Populace control** 13-6, 13-3, 14-14b 14-4

**Port security** 12-16d 12-16

**Private document source** 6-9 6-3

**Priority target** 12-8 12-4

**Progressive surveillance** 4-27d 4-23

**Protection of:**

**Of investigative reports** 7-4, 11-3 7-2, 11-2

**Of sources** 6-4, 6-5, 6-1, 6-2, app B B-1
<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personnel</td>
<td>10-11, app E 10-6, E-1</td>
</tr>
<tr>
<td>Physical</td>
<td>10-12, 11-2, 10-7, 12-16d, 11-1, 13-5 12-16, 13-2</td>
</tr>
<tr>
<td>Port and harbor</td>
<td>12-16d, 14-11f 12-16, 14-3</td>
</tr>
<tr>
<td>Rear area services</td>
<td>12-5b 12-3</td>
</tr>
<tr>
<td>Troop movement</td>
<td>12-12eí, 14-11/ 12-16, 14-3</td>
</tr>
<tr>
<td>Selection, target</td>
<td>12-8 12-4</td>
</tr>
<tr>
<td>Sensors, unattended ground</td>
<td>12-3b 12-1</td>
</tr>
<tr>
<td>Sheet, key (fig B-7)</td>
<td>app B B-1</td>
</tr>
<tr>
<td>Signal:</td>
<td>14-15 14-4</td>
</tr>
<tr>
<td>Security</td>
<td>10-12d 10-7</td>
</tr>
<tr>
<td>Social Security Administration, US</td>
<td>4-5f 4-3</td>
</tr>
<tr>
<td>Sources:</td>
<td>6-4b 6-2</td>
</tr>
<tr>
<td>Casual</td>
<td>6-5 6-2</td>
</tr>
<tr>
<td>Confidential</td>
<td>6-4, 7-7, 6-1, 7-9, app B B-1</td>
</tr>
<tr>
<td>Documentary</td>
<td>6-6, 13-13b 6-2, 12-13, 13-11</td>
</tr>
<tr>
<td>Human</td>
<td>6-3 6-1</td>
</tr>
<tr>
<td>Incidental</td>
<td>6-4a 6-1</td>
</tr>
<tr>
<td>Mass media</td>
<td>6-7 6-2</td>
</tr>
<tr>
<td>Material</td>
<td>6-10 6-3</td>
</tr>
<tr>
<td>Official</td>
<td>6-4c, 13-13b 6-2, 13-11</td>
</tr>
<tr>
<td>On drugs</td>
<td>app E E-1</td>
</tr>
<tr>
<td>Personnel document</td>
<td>6-9 6-3</td>
</tr>
<tr>
<td>Political</td>
<td>13-13b 13-11</td>
</tr>
<tr>
<td>Private documents</td>
<td>6-9 6-3</td>
</tr>
<tr>
<td>Religious</td>
<td>13-13b 13-11</td>
</tr>
<tr>
<td>Scientific</td>
<td>6-8 6-3</td>
</tr>
<tr>
<td>Technical</td>
<td>6-8, 6-10 6-3</td>
</tr>
<tr>
<td>Unwitting</td>
<td>6-4a 6-1</td>
</tr>
<tr>
<td>Walk-ins</td>
<td>4-13a 4-9</td>
</tr>
<tr>
<td>Special:</td>
<td>1-2, 4-36 1-1, 4-30</td>
</tr>
<tr>
<td>Agent</td>
<td>2-6 2-3</td>
</tr>
<tr>
<td>Counterintelligence units</td>
<td>1-3c, 12-16d 1-2, 12-16</td>
</tr>
<tr>
<td>Operations</td>
<td>12-12</td>
</tr>
<tr>
<td>Special weapons security</td>
<td>12-3b, 12-12d 12-1, 12-12</td>
</tr>
<tr>
<td>Specialist, Counterintelligence</td>
<td>1-2 1-1</td>
</tr>
<tr>
<td>Spot Report</td>
<td>7-11 7-3</td>
</tr>
<tr>
<td>Spying</td>
<td>9-11 9-4</td>
</tr>
<tr>
<td>Stability operations</td>
<td>13-1 13-1</td>
</tr>
<tr>
<td>Standard Operating Procedures (SOP)</td>
<td>13-5 13-2</td>
</tr>
<tr>
<td>Statement, sworn</td>
<td>3-12, 4-14 3-8, 4-10</td>
</tr>
<tr>
<td>Contents</td>
<td>3-15 3-8</td>
</tr>
<tr>
<td>Formal (fig 3-2, 3-3, 3-4)</td>
<td>3-18 3-10</td>
</tr>
<tr>
<td>In foreign countries</td>
<td>3-23, 3-24 3-11</td>
</tr>
<tr>
<td>Opinions and conclusions</td>
<td>3-21 3-10</td>
</tr>
<tr>
<td>Other than direct testimony</td>
<td>3-20 3-10</td>
</tr>
<tr>
<td>Preparation of</td>
<td>3-13, 3-13, 3-8, 3-22, 3-28 3-10—</td>
</tr>
<tr>
<td>Use of</td>
<td>3-14 3-8</td>
</tr>
<tr>
<td>Statutes:</td>
<td>9-9 9-3</td>
</tr>
<tr>
<td>Espionage</td>
<td>9-14 9-5</td>
</tr>
<tr>
<td>Liaison</td>
<td>5-15d, app E 5-9, E-1</td>
</tr>
<tr>
<td>Subject Interview</td>
<td>3-6e, 4-12 3-2, 4-8</td>
</tr>
<tr>
<td>Subversive activity</td>
<td>9-23, 14-4c, 9-8, 14-5, 14-11b, 14-1, 14-14e, 14-3, 14-14g 14-4</td>
</tr>
<tr>
<td>Suitability</td>
<td>8-19a 8-5</td>
</tr>
<tr>
<td>Summary of Information (SOI):</td>
<td>7-8, app B B-1</td>
</tr>
<tr>
<td>Format (fig B-9)</td>
<td>7-3</td>
</tr>
<tr>
<td>Characterization—Individual (fig B-10, B-12)</td>
<td>app B B-1</td>
</tr>
<tr>
<td>Characterization—Organization (fig B-11)</td>
<td>app B B-1</td>
</tr>
<tr>
<td>Surreptitious entry</td>
<td>5-26, 5-6 5-1, 5-5</td>
</tr>
<tr>
<td>Survey, counterintelligence</td>
<td>10-1 10-1</td>
</tr>
<tr>
<td>Checklist</td>
<td>10-4, app D 10-2, D-1</td>
</tr>
<tr>
<td>Initiation</td>
<td>10-2 10-1</td>
</tr>
<tr>
<td>Preparation</td>
<td>10-3 10-2</td>
</tr>
<tr>
<td>Report</td>
<td>10-17, app C 10-9, C-1</td>
</tr>
<tr>
<td>Surveillance</td>
<td>4-23 4-15</td>
</tr>
<tr>
<td>ABC method (fig 4-1)</td>
<td>4-27b 4-18</td>
</tr>
<tr>
<td>AB method (fig 4-2)</td>
<td>4-27b 4-18</td>
</tr>
<tr>
<td>Audio</td>
<td>5-2a, 5-3 5-1, 5-2</td>
</tr>
<tr>
<td>Checkpoint</td>
<td>4-27d 4-18</td>
</tr>
<tr>
<td>Close</td>
<td>4-25c 4-15</td>
</tr>
<tr>
<td>Combination or mixed</td>
<td>4-25b 4-16</td>
</tr>
<tr>
<td>Communications</td>
<td>4-26f 4-18</td>
</tr>
<tr>
<td>Compromise</td>
<td>4-28k 4-25</td>
</tr>
<tr>
<td>Detecting</td>
<td>4-29 4-25</td>
</tr>
<tr>
<td>Discreet</td>
<td>4-25a 4-15</td>
</tr>
<tr>
<td>Eluding</td>
<td>4-30 4-28</td>
</tr>
<tr>
<td>Encounters with friends</td>
<td>4-29c 4-23</td>
</tr>
<tr>
<td>Equipment</td>
<td>5-4 5-2</td>
</tr>
<tr>
<td>Fixed</td>
<td>4-25b, 4-26a 4-16</td>
</tr>
<tr>
<td>Moving</td>
<td>4-25b, 4-26a 4-16</td>
</tr>
<tr>
<td>Objectives</td>
<td>4-24 4-15</td>
</tr>
<tr>
<td>One-man/vehicular method</td>
<td>4-27b 4-18</td>
</tr>
<tr>
<td>Personnel selection</td>
<td>4-26e 4-16</td>
</tr>
<tr>
<td>Preparation for</td>
<td>4-26 4-16</td>
</tr>
<tr>
<td>Progressive</td>
<td>4-27d 4-23</td>
</tr>
<tr>
<td>Team commander</td>
<td>4-26d 4-17</td>
</tr>
<tr>
<td>Technical</td>
<td>4-25b 4-16</td>
</tr>
<tr>
<td>Techniques</td>
<td>4-28 4-23</td>
</tr>
<tr>
<td>Types</td>
<td>4-25 4-25</td>
</tr>
<tr>
<td>Use of indigenous personnel</td>
<td>4-26d 4-17</td>
</tr>
<tr>
<td>Vehicular (fig 4-1, 4-2, 4-3)</td>
<td>4-27b 4-18</td>
</tr>
<tr>
<td>Survey, physical security</td>
<td>app D D-1</td>
</tr>
<tr>
<td>Survey, technical:</td>
<td>11-3 11-2</td>
</tr>
<tr>
<td>Conduct of</td>
<td>11-5 11-2</td>
</tr>
<tr>
<td>Equipment</td>
<td>app C C-1</td>
</tr>
<tr>
<td>Report</td>
<td></td>
</tr>
</tbody>
</table>
### Index

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspect:</td>
<td></td>
</tr>
<tr>
<td>Interrogation</td>
<td>4-17, 9-7b 4-12, 9-2</td>
</tr>
<tr>
<td>Rights of</td>
<td>3-6, 4-12a 3-2, 4-8</td>
</tr>
<tr>
<td>Civilian</td>
<td>3-6d 3-3</td>
</tr>
<tr>
<td>Military</td>
<td>3-6d 3-3</td>
</tr>
<tr>
<td>Sworn Statement</td>
<td>3-12, 4-14 3-8, 4-10</td>
</tr>
<tr>
<td>Contents</td>
<td>3-15 3-8</td>
</tr>
<tr>
<td>Formal (fig 3-2, 3-3, 3-4)</td>
<td>3-18 3-10</td>
</tr>
<tr>
<td>In foreign countries</td>
<td>3-22, 3-24 3-11</td>
</tr>
<tr>
<td>Opinions and conclusions</td>
<td>3-21 3-10</td>
</tr>
<tr>
<td>Other than direct testimony</td>
<td>3-20 3-10</td>
</tr>
<tr>
<td>Preparation of</td>
<td>3-13, 3-18, 3-22, 3-10— 3-28 3-12</td>
</tr>
<tr>
<td>Unsigned</td>
<td>3-27 3-11</td>
</tr>
<tr>
<td>Unsworn</td>
<td>3-26, 4-17 3-11, 4-12</td>
</tr>
<tr>
<td>Use of</td>
<td>3-14 3-8</td>
</tr>
<tr>
<td>Tactical operations</td>
<td>12-4, 12-5, 12-2— 12-6, 12-15 12-4, 12-12</td>
</tr>
<tr>
<td>Tactical troop augmentation</td>
<td>12-10a 12-6</td>
</tr>
<tr>
<td>&quot;Tapping&quot;</td>
<td>5-5 5-4</td>
</tr>
<tr>
<td>Target, counterintelligence:</td>
<td></td>
</tr>
<tr>
<td>Document and material</td>
<td>12-9d 12-6</td>
</tr>
<tr>
<td>Files</td>
<td>12-10e 12-7</td>
</tr>
<tr>
<td>Installation</td>
<td>12-9b 12-5</td>
</tr>
<tr>
<td>Lists</td>
<td>12-4a 12-2</td>
</tr>
<tr>
<td>Organization and group</td>
<td>12-9c 12-6</td>
</tr>
<tr>
<td>Personalities</td>
<td>12-9a, 12-11b 12-5, 12-8</td>
</tr>
<tr>
<td>Records</td>
<td>12-10c 12-7</td>
</tr>
<tr>
<td>Selection and priorities</td>
<td>12-8 12-4</td>
</tr>
<tr>
<td>Technical:</td>
<td></td>
</tr>
<tr>
<td>Inspection</td>
<td>11-1b, 11-2d, 11-1, 11-3b 11-2</td>
</tr>
<tr>
<td>Intelligence</td>
<td>6-11, 14-15 6-3, 14-4</td>
</tr>
<tr>
<td>Source</td>
<td>6-8, 6-10 6-3</td>
</tr>
<tr>
<td>Surveillance</td>
<td>4-25b 4-16</td>
</tr>
<tr>
<td>Survey</td>
<td>11-1a, 11-2c, 11-1, 11-3a 11-2</td>
</tr>
<tr>
<td>Technicians, counterintelligence</td>
<td>1-2 1-1</td>
</tr>
<tr>
<td>Techniques:</td>
<td></td>
</tr>
<tr>
<td>Investigative</td>
<td>4-3 4-1</td>
</tr>
<tr>
<td>Surveillance</td>
<td>4-28 4-23</td>
</tr>
<tr>
<td>Termination of interview</td>
<td>4-13b 4-9</td>
</tr>
<tr>
<td>Testimony</td>
<td>4-37 4-31</td>
</tr>
<tr>
<td>Theater Army</td>
<td>2-7a, 2-8a 2-3, 2-4</td>
</tr>
<tr>
<td>&quot;Third Agency Rule&quot;</td>
<td>6-15b, app B 6-4, B-1</td>
</tr>
<tr>
<td>&quot;Throw-offs&quot;</td>
<td>4-11i, app B 4-7, B-1</td>
</tr>
<tr>
<td>Tranquilizers</td>
<td>app E E-1</td>
</tr>
<tr>
<td>Transfer of documents</td>
<td>12-4a 12-2</td>
</tr>
<tr>
<td>Translators:</td>
<td></td>
</tr>
<tr>
<td>Qualifications and use of</td>
<td>12-12a 12-10</td>
</tr>
<tr>
<td>Used with statements</td>
<td>3-24 3-11</td>
</tr>
<tr>
<td>Working with</td>
<td>13-11 13-9</td>
</tr>
<tr>
<td>Transmittal of evidence</td>
<td>4-34a 4-29</td>
</tr>
<tr>
<td>Treason</td>
<td>9-13 9-5</td>
</tr>
<tr>
<td>Troop Movement Security</td>
<td>12-12c 12-11</td>
</tr>
<tr>
<td>Type:</td>
<td></td>
</tr>
<tr>
<td>Records</td>
<td>4-4a, 4-5, 4-2</td>
</tr>
<tr>
<td>Sabotage</td>
<td>9-6 9-2</td>
</tr>
<tr>
<td>Surveillance</td>
<td>4-24 4-15</td>
</tr>
<tr>
<td>Unattended ground sensors</td>
<td>12-3b 12-1</td>
</tr>
<tr>
<td>Units, special counterintelligence</td>
<td>2-6 2-3</td>
</tr>
<tr>
<td>Unannounced counterintelligence</td>
<td></td>
</tr>
<tr>
<td>inspection</td>
<td>10-16b 10-8</td>
</tr>
<tr>
<td>Units, special counterintelligence</td>
<td>2-6 2-3</td>
</tr>
<tr>
<td>Unlawfully obtained evidence</td>
<td>3-9 3-8</td>
</tr>
<tr>
<td>Unwitting source</td>
<td>6-4a 6-1</td>
</tr>
<tr>
<td>US Army Security Agency</td>
<td>4-32b, 10-1d, 4-27, 10-12d, 11-2, 10-1, 12-11e 10-7, 11-1, 12-8</td>
</tr>
<tr>
<td>US Government, advocating overthrow</td>
<td>9-19 9-7</td>
</tr>
<tr>
<td>Waiver</td>
<td>3-6a, 3-6f, 3-2, 3-4, 3-17, 3-9, 4-17d 4-15</td>
</tr>
<tr>
<td>&quot;Walk-ins&quot;</td>
<td>4-13a, 6-4a 4-9, 6-1</td>
</tr>
<tr>
<td>Warrant, search:</td>
<td></td>
</tr>
<tr>
<td>Civilian</td>
<td>3-7d 3-7</td>
</tr>
<tr>
<td>Military</td>
<td>3-7c 3-7</td>
</tr>
<tr>
<td>White list</td>
<td>12-9a, 12-11b 12-5, 12-8</td>
</tr>
<tr>
<td>Witness:</td>
<td></td>
</tr>
<tr>
<td>Arrangements for</td>
<td>5-17e 5-9</td>
</tr>
<tr>
<td>Evaluation</td>
<td>4-15 4-12</td>
</tr>
<tr>
<td>Interview</td>
<td>4-14 4-10</td>
</tr>
<tr>
<td>Special Agent</td>
<td>4-36, 4-38 4-30, 4-31</td>
</tr>
<tr>
<td>Writing, secret</td>
<td>4-32e, 5-2d, 4-27, 5-10b 5-2, 5-7</td>
</tr>
</tbody>
</table>
By Order of the Secretary of the Army:

W. C. WESTMORELAND,
General, United States Army,
Chief of Staff.

Official:
VERNE L. BOWERS,
Major General, United States Army,
The Adjutant General.

Distribution:
To be distributed in accordance with DA Form 12–11 requirements for Counterintelligence Operations, Intelligence Corps, US Army.