

9 January 2010

Operations and Signal Security
OPERATIONS SECURITY (OPSEC)

***This regulation supersedes Eighth Army Regulation 530-1, 20 July 2001.**

FOR THE COMMANDER:

LEWIS F. SETLIFF
Colonel, GS
Chief of Staff

Official:



GARRIE BARNES
Chief, Publications and
Records Management

Summary. This regulation prescribes policies, responsibilities, supply and logistical procedures related to ACL, wartime planning, training and miscellaneous activities to be used by 8th Army units, off-shore units training in Korea and activities supported by 8th Army.

Summary of Change. This document has been substantially changed. A full review of its content is required.

Applicability. This regulation applies to all personnel and all Army units assigned to Headquarters (HQ) 8th Army, off shore Army units training in Korea and units located in Korea supported by inter-service support agreements with HQ 8th Army.

Supplementation. Supplementation of this regulation and issuance of command and local forms is prohibited unless prior approval is obtained from HQ 8th Army, OMD, OPSEC Officer, Unit #15236, APO AP 96205-5236.

Forms. AK forms are available at http://8tharmy.korea.army.mil/g1_AG/Programs_Policy/Publication_Records_Forms.htm.

Records Management. Records created as a result of processes prescribed by this regulation must be identified, maintained and disposed of according to AR 25-400-2. Record titles and descriptions are available on the Army Records Information System website at <https://www.arims.army.mil>.

Suggested Improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQ Eighth Army OMD Operations, ATTN: OPSEC Officer, APO AP 96204-0027.

Distribution. Electronic Media Only (EMO).

Distribution Restriction Statement. This publication contains technical or operational information that is for official Government use only. Distribution is limited to U.S. Government agencies and their contractors. Requests from outside U.S. Government agencies for release of this publication under the Freedom of Information Act or the Foreign Military Sales Program must be made to HQ, 8th Army OMD Operations, ATTN: OPSEC Officer, PSC 303 Box 27, APO AP 96204-0027

Destruction Notice. Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

CONTENTS

Chapter 1

Introduction, page 1

- 1-1. Purpose
- 1-2. References
- 1-3. Explanation of Abbreviations and Terms
- 1-4. Requirements
- 1-5. Application
- 1-6. Proponent

Chapter 2

Responsibilities, page 3

- 2-1. 8th Army Commander
- 2-2. All Commanders
- 2-3. Primary 8th Army Staff Sections and Chiefs of Special Staffs
- 2-4. 8th Army OSD- Personnel (G1)
- 2-5. 8th Army OID (G2)
- 2-6. 8th Army OMD (G3/5/7)
- 2-7. 8th Army OSD-Logistics (G4)
- 2-8. 8th Army OCCD (G6)
- 2-9. 8th Army CMO (G9)
- 2-10. The Inspector General (IG)
- 2-11. Public Affairs Office (PAO)
- 2-12. All Army personnel

Chapter 3

Policy and Procedures, page 6

- 3-1. General
- 3-2. OPSEC Programs
- 3-3. Threat Analysis Support to OPSEC

Chapter 4

Training Requirements, page 9

- 4-1. Overview
- 4-2. Training Programs

Chapter 5

OPSEC Review, Assessment and Survey, page 10

Section I. OPSEC Review

- 5-1. General
- 5-2. Procedures

Section II. OPSEC Assessment

- 5-3. General
- 5-4. Procedures

CONTENTS (Cont')

Section III. OPSEC Survey

- 5-5. General
- 5-6. Planning phase
- 5-7. Field survey phase
- 5-8. Analysis and reporting phase

Appendixes, page 18

- A. References
- B. OPSEC Indicators
- C. Sample Questions for CIL
- D. OPSEC Relations to Other Programs
- E. The Threat
- F. OPSEC Assessment
- G. Forms and Worksheets
- H. OPSEC Working Group

Figure Lists

- Figure 5-1. OPSEC survey sequence of actions, *page 12*
- Figure 5-2. Generic Functional Outline/Profile The completed profile gives a picture of the functional area, *page 14*
- Figure 5-3. Example OPSEC Survey Report Format, *page 17*

Glossary, page 36

Chapter 1

Introduction

1-1. Purpose

To establish policy and procedures for Operations Security (OPSEC) within the 8th Army, its subordinate, and supporting commands.

1-2. References

Required and related publications are listed in Appendix A.

1-3. Explanation Of Abbreviations and Terms

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

1-4. Requirement

a. The National Operations Security (OPSEC) Program (National Security Division Decision Directive 298) requires each executive department and agency with a national security mission to have an OPSEC program. DODD 5205.02 supports the national program and requires each DOD component to have an OPSEC program.

b. Operations security maintains essential secrecy, which is the condition achieved by the denial of critical information to adversaries. Adversaries in possession of critical information can hinder or prevent friendly mission accomplishment. Thus, essential secrecy is a necessary prerequisite for effective operations. Essential secrecy depends on the combination of two approaches to protection:

(1) Traditional security programs to deny adversaries classified information.

(2) Operations security to deny adversaries critical information, which is always sensitive and often unclassified.

c. Operations security provides methodology to manage risk. It is impossible to avoid all risk and protect everything. To attempt complete protection diverts resources from actions needed for mission success.

1-5. Application

a. Operations security awareness and execution is crucial to Army success. OPSEC is applicable to all personnel and all 8th Army missions and supporting activities on a daily basis. OPSEC denies adversaries information about friendly capabilities, activities, limitations, and intentions that adversaries need to make competent decisions. Without prior knowledge of friendly actions, adversary leaders cannot act effectively to prevent friendly mission accomplishment. It applies to all Army activities and is required during training, sustaining, mobilizing, preparing for, and conduction operations, exercises, tests, or activities.

(1) The 8th Army OPSEC program is consistent with the Army OPSEC program, joint policy and doctrine in Chairman, Joint Chiefs of Staff Instruction (CJCSI) 3213.01B and Joint Publication 3-13.3. In Joint and Army operations, OPSEC is a core capability of IO as prescribed in JP 3-13.3 and FM 3-13.

(2) Information Operations (IO) core capabilities integrates OPSEC, military deception,

psychological operations (PSYOP), electronic warfare (EW), and computer network defense. The IO supporting capabilities include information assurance (IA), counterintelligence (CI), and physical destruction; while related activities that are integrated include public affairs and civil military operations. All of these capabilities deny information to, influence, degrade, or destroy enemy command, control, communications, computers, and intelligence (C4I) capabilities while protecting friendly C4I capabilities against similar actions.

(3) Operations security contributes directly to the unit's ability to field forces superior to an adversary in peace, crisis, or war. Without critical information about our forces, adversaries cannot design and build systems, devise tactics, train, or otherwise prepare their forces (physically or psychologically) in time to effectively counter 8th Army capabilities or intentions.

b. Operations security is more important now than it has ever been. The U.S. faces cunning and ruthless adversaries fighting asymmetrically to avoid our strengths. The first step for them to inflict harm is to gather information about us. They are exploiting the openness and freedoms of our society by aggressively reading and collecting material that is needlessly exposed to them. Good OPSEC practices can prevent these compromises and allow us to maintain essential secrecy about our operations.

1-6. Proponent

The Assistant Chief of Staff (ACoS) G3/5/7 is the 8th Army proponent for OPSEC. Subsequently, the command, unit, or installation operations officer is the staff proponent for OPSEC. However, the success or failure of OPSEC is ultimately the responsibility of the Commander and the most important emphasis for implementing OPSEC comes from the chain of command.

a. Operations security is an operations function that protects critical information and requires close integration with other security programs.

b. A unit Commander, operations officer, and the OPSEC Officer must consider OPSEC in all unit activities to maintain operational effectiveness.

(1) Unit actions are a primary source of indicators collected by adversaries. The Commander, advised by the OPSEC Officer, controls these actions, assigns tasks, and allocates resources to implement OPSEC measures.

(2) By constantly observing activities, the OPSEC Officer can evaluate these measures for their effectiveness and their impact on operational success.

c. While the OPSEC Officer is responsible for the development, organization, and administration of an OPSEC program, the Commander's emphasis and support from the chain of command is essential to ensure the proper implementation of an OPSEC program.

Chapter 2 Responsibilities

2-1. 8th Army Commander

8th Army commander will develop and implement a functioning, active, and documented (formal) OPSEC program. To develop and implement a formal OPSEC program, the 8th Army commander will-

a. Appoint a Command OPSEC program manager in writing.

(1) The 8th Army OPSEC program manager is responsible for numerous OPSEC programs within the command and provides guidance and oversight, and coordinates their actions under the Command's OPSEC program. Dependent on the workload, supporting staff may be necessary to assist the Command's OPSEC program manager.

(2) The individual will be an experienced commissioned officer (at least a Major/O-4 or a CW3), noncommissioned officer (Sergeant Major) or DA Civilian equivalent. The Commander, or designated authority, can approve an exception to these rank/grade levels.

(3) Because contractors do not have authority over U.S. military and government personnel and cannot represent the position of the U.S. Government, contract employees will not be assigned as the command's OPSEC program manager or OPSEC officer. However, they may perform OPSEC duties in a supporting capacity as the OPSEC coordinator.

b. Develop and implement functioning, active, and documented (formal) OPSEC programs for staff organizations within the command to meet their specific needs and to support the command's OPSEC program.

c. Ensure 8th Army OPSEC program manager maintain routine contact with the Army and USFK OPSEC program managers. The 8th Army OPSEC program manager will provide updates, status reports, OPSEC issues, OPSEC compromises, lessons learned, initiatives, requests for support, recommendations, personnel turnover, verification of contact information, media contacts, and so forth.

d. Submit the 8th Army Annual OPSEC Report for the fiscal year (FY) to the Army OPSEC Support Element (OSE). Guidance for format and a submission suspense date will be provided by the Army OPSEC program manager.

e. Ensure the 8th Army OPSEC programs are examined as part of the Command Inspection Program (CIP) as outlined in AR 1-201 and AK Pam 1-201.

f. According to AR 530-1, Paragraph 2-4, " Commanders of Army Commands, Army Service Component Commands and Direct Reporting Units. Ensure that their tenant units coordinate with the garrison OPSEC Officer and participate in the garrison installation-level OPSEC working groups as require.

g. Ensure OPSEC annual training is conducted by subordinate and supporting commands in order to maintain a high level of OPSEC awareness.

h. Identify and resource additional OPSEC personnel requirements as required.

- i. Participate in HQDA-level Integrated Planning Team (IPT) OPSEC conferences.

2-2. All Commanders

a. OPSEC is a command responsibility. Commanders and agency heads will ensure that their organizations plan and implement appropriate OPSEC measures to preserve essential secrecy in every phase of an operation, exercise, test, or activity.

b. Appoint an OPSEC Officer in writing with responsibility for supervising the execution of proper OPSEC within their organization. This appointment may be an additional duty.

c. Commanders will develop and implement OPSEC programs to meet their specific needs and to support the OPSEC programs. They will-

(1) Ensure that the appointed OPSEC Officer receives appropriate training in accordance with chapter 4 of this regulation, and that they are of sufficient rank or grade to execute their responsibilities.

(2) Establish OPSEC as a command emphasis item and include OPSEC effectiveness as an evaluation objective for exercises, operations, and activities.

(3) Approve the organization's Critical Information List (CIL). Circulate the list to all subordinates as widely as security classification permits.

(4) Establish a documented OPSEC program that includes as a minimum, OPSEC Officer appointment orders and OPSEC SOP. At a minimum, the OPSEC standing operating procedure (SOP) should include the unit or activity's critical information and OPSEC measures to protect it.

(5) Commanders may mandate at a minimum that their subordinate commands determine their critical information, develop OPSEC measures to protect their critical information, and provide this information to a higher echelon OPSEC program.

(6) In accordance with AR 530-1, Paragraph 2-4. 8th Army and subordinate units will participate in garrison installation-level OPSEC working groups as required.

2-3. 8th Army Staff Directorates and Chiefs of Special Staffs

Each staff section will designate an OPSEC officer to coordinate OPSEC-related matters with the 8th Army OPSEC program manager. The individual may be a commissioned officer (MAJ or above), warrant officer, (CW3 or above), noncommissioned officer (SFC or above), or a Department of the Army (DA) civilian equivalent.

2-4. 8th Army OSD-Personnel (G1)

a. The OSD-PER will ensure that personnel actions do not jeopardize the Army's OPSEC posture.

b. Be familiar with regulations pertaining to the disclosure of personal and FOUO information to prevent the release of information that could place the unit and/or soldier in jeopardy.

2-5. 8th Army OID (G2)

- a. Assist other 8th Army staff agencies in the development of doctrine and in the preparation of training programs pertinent to all intelligence, counterintelligence and security aspects of OPSEC.
- b. Provide overall threat assessment to forces in addition to threat assessment to specific operations.
- c. Be the 8th Army staff proponent for signal intelligence (SIGINT), human intelligence (HUMINT), imagery intelligence (IMINT), measurement & signal intelligence (MASINT), and open source intelligence (OSINT) supporting OPSEC.
- d. Recommend OPSEC measures.

2-6. 8th Army OMD (G3/5/7)

- a. Budget for OPSEC activities to include operations, exercises, OPSEC surveys and evaluations, training and assistance, and conferences as necessary.
- b. Request training and survey services from the Inter-Agency OPSEC Support Staff (IOSS) and submit request through HQ USFK CJ39.
- c. Ensure appropriate OPSEC measures are taken within 8th Army to preserve essential secrecy.
- d. Publish protective measures to be implemented in Operation Plans and Operation Orders.
- e. Ensure OPSEC training is conducted IAW regulations and doctrine.
- f. Serve as chairperson during OPSEC Working Groups.

2-7. 8th Army OSD-Logistics (G4)

- a. Analyze logistics reports and procedures to identify indicators compromising 8th Army intent and/or logistical status. Logistical operations such as port and airfield activity can be prime indicators of future operations.
- b. Limit release of transportation arrangements and plans to only minimal sources required to plan and complete the mission.

2-8. 8th Army OCCD (G6)

- a. Assist the OID and OMD in developing the Command and Control (C2) appendix for 8th Army OPLANS, CONPLANS and exercise directives.
- b. Establish emission control and wartime reserve modes for 8th Army communication emitters.
- c. Enforce procedures for password and login protection.

d. Act as 8th Army executive agent for information assurance (IA) and Computer Network Defense (CND).

2-9. 8th Army CMO (G9)

a. Assist the OID in recognizing possible human intelligence (HUMINT) activities supporting OPSEC (i.e. any information pertaining to OPSEC issues).

b. Ensure G9 personnel have a strong understanding of OPSEC prior to dealing with outside sources (NGOs, etc.) in the conduct of mission.

2-10. The Inspector General (IG)

The Inspector General will ensure that OPSEC is an item of interest in inspections of organizations throughout 8th Army.

2-11. Public Affairs Office (PAO)

a. Ensure that OPSEC has been considered in the preparation of all public releases of information.

b. Conduct prior coordination with the OPSEC Officer and PSYOP representative before releasing operational or mission related information to prevent disclosure of essential information.

c. Assist the OID in recognizing possible open source intelligence (OSINT) activities supporting OPSEC (i.e. any information pertaining to OPSEC issues).

2-12. All Army Personnel

a. All 8th Army personnel (active component, reserve component, DA civilians), and civilian contractors will implement OPSEC measures as determined by the commander or OPSEC Officer to protect sensitive and critical information from unauthorized disclosure.

b. Handle any attempt by unauthorized personnel to solicit sensitive or critical information as a SAEDA incident per AR 381-12. Report all facts immediately to the nearest supporting counterintelligence office and inform the chain of command. If counterintelligence offices are not readily available, report such incidents to the organizational security manager or to the unit commander.

c. Be familiar with AR 340-21 to prevent disclosure of personal or private information.

Chapter 3 Policy and Procedures

3-1. General

Operations Security applies throughout the range of operations across the spectrum of conflict to all 8th Army operations. All 8th Army MSCs will have functional, active, and documented OPSEC programs. These programs will use the process described in this chapter to identify and protect critical information.

3-2. OPSEC Programs

A functional, active, and documented OPSEC program will have the following common features: an OPSEC Program Manager or OPSEC Officer appointed in writing; the use of the five-step OPSEC process; an OPSEC SOP to document the unit, activity, installation, or staff organization's critical information and OPSEC measures to protect it; and the coordination of OPSEC with other security programs.

a. An OPSEC program has an OPSEC program manager or OPSEC officer appointed in writing.

(1) An OPSEC program manager is responsible for the development, organization, and administration of an OPSEC program. The OPSEC program manager provides guidance and oversight to multiple subordinate OPSEC programs of various units, activities, and organizations and coordinates their actions under the Command's OPSEC program. OPSEC program managers are also OPSEC officers, but because of the extent and complexity of the OPSEC program they oversee, they are primarily referred to as OPSEC program managers.

(2) An OPSEC officer is responsible for the development, organization, and administration of an OPSEC program at division level and below.

(3) While the OPSEC program manager or OPSEC officer is responsible for the development, organization, and administration of an OPSEC program, the commander's emphasis and support from the chain of command is essential to ensure the proper implementation of an OPSEC program.

(a) The appropriate rank/grade level for OPSEC program managers and OPSEC officers is as follows:

(b) 8th Army: an experienced commissioned officer (at least a Major/O-4 or a CW3), noncommissioned officer (Sergeant Major) or DA Civilian equivalent.

(c) Division: Captain (O-3) or above, Warrant Officer (CW2 or above), Noncommissioned Officer (E-8 or above), or DA Civilian equivalent.

(d) Brigade: Captain (O-3) or above, Warrant Officer, Noncommissioned Officer (E-7 or above), or DA Civilian equivalent.

(e) Battalion: First Lieutenant (O-2) or above, Warrant Officer, Noncommissioned Officer (E-6 or above) or DA Civilian equivalent.

(f) Below Battalion level: Any Officer, Warrant Officer, Noncommissioned Officer (E-5 or above) or DA Civilian equivalent as required.

(g) The Commander, or designated authority, can approve an exception to the rank/grade levels listed above.

(h) Because contractors do not have authority over U.S. military and government personnel, contract employees will not be assigned as the command's primary OPSEC program manager or OPSEC officer. However, they may perform OPSEC duties in a supporting capacity.

(4) Operations security program managers and OPSEC officers will receive appropriate training for their duty positions. (See chap 4.)

b. An OPSEC program utilizes the five-step OPSEC process.

(1) The OPSEC process can apply to any plan, operation, program, project, or activity. It provides a framework for the systematic process necessary to identify and protect critical information. The process is continuous. It considers the changing nature of critical information, the threat and vulnerability assessments throughout the operation. It uses the following steps:

(a) Identification of critical information – determine what information needs protection.

(b) Analysis of threats – identify the adversaries and how they can collect information.

(c) Analysis of vulnerabilities – analyze what critical information friendly forces are exposing.

(d) Assessment of risk – assess what protective measures should be implemented.

(e) Application of appropriate OPSEC measures – countermeasures that protect critical information.

(2) Refer to appendix B for more details of the five-step OPSEC process.

c. An OPSEC policy letter and/or SOP, at a minimum documents the unit or staff organization's critical information list (CIL) and OPSEC protection measures.

(1) The OPSEC SOP can include more information such as a threat analysis and a list of potential vulnerabilities.

(2) The most important items that personnel must know from the SOP are the unit or organization's critical information list and OPSEC measures.

(3) As a general rule, it is best to keep the number of items of critical information list to fewer than 10 in order to aid in simplicity.

(4) Personnel must know the unit's OPSEC measures and practice them on a consistent and continuous basis. The OPSEC Officer should see that training of implementing OPSEC measures be included in organization's annual training.

d. The OPSEC program must be coordinated and synchronized with the command's other security programs such as information security (INFOSEC), information assurance (IA), physical security, force protection, etc. This ensures that the security programs do not provide conflicting guidance and work together to support each other.

3-3. Threat analysis support to OPSEC

The intelligence staff of the command will provide threat analysis in support of OPSEC. When this is not practical or possible, forward requirements through proper channels to the appropriate threat analysis center.

Chapter 4 Training Requirements

4-1. Overview

For OPSEC to be effective, all Army personnel (Soldier, DA Civilian, and DOD contractors) must be aware of OPSEC and understand how OPSEC complements traditional security programs. All personnel must know how to apply and practice OPSEC in the performance of their daily tasks. OPSEC must become a mindset of all Army personnel and be performed as second nature. To accomplish this level of OPSEC vigilance, OPSEC training programs must be action and job-oriented, enabling the workforce to put into practice the knowledge and tactics, techniques, and procedures (TTPs) they learned in training. Training should maximize the use of lessons learned to illustrate OPSEC objectives and requirements. In order to ensure accomplishment of training, commanders will include OPSEC training as a part of their organization's annual training guidance.

4-2. Training programs

Commanders will ensure their appointed OPSEC officers and program managers attend formal OPSEC resident training using a combination of resident or mobile training team (MTT) courses to accomplish the three levels of OPSEC training outlined below:

a. *Operations Security Level I Training.* The target audience is all Army personnel (the total workforce consisting of Soldiers, DA Civilians, and DOD contractors). Level I training is composed of both initial and continual awareness training:

(1) *Initial Operations Security Awareness Training.* All newly assigned personnel within the first 30 days of arrival in the organization must receive initial training. It is recommended that this training be conducted as part of an initial entry briefing or unit newcomer's briefings. This training is provided by the unit OPSEC officer. The intent and focus of initial training will be on the following areas:

(a) Understanding the difference between OPSEC and other security programs and how OPSEC complements traditional security programs to maintain essential secrecy of U.S. military capabilities, intentions, and plans.

(b) Understanding what is critical information.

(c) How adversaries aggressively seek information on U.S. military capabilities, intentions, and plans.

(d) Specific guidance on how to protect critical information through OPSEC measures.

(e) Endstate: Each individual should have the requisite knowledge to safeguard critical information and know the answers to the following questions:

- What is my unit's critical information?
- What critical information am I personally responsible for protecting?
- How is the threat trying to acquire my critical information?
- What steps am I/are we taking to protect my/our critical information?

- Who is my OPSEC Officer (in order to report an OPSEC concern, compromise, or ask an OPSEC question)?

b. *Operations Security Level II Training.* The appointed OPSEC program manager or OPSEC officer will attend the DOD OPSEC Course (OPSE-2500) conducted by the Joint Information Operations Warfare Command (JIOWC) or an OPSEC program manager certified by the OPSEC Support Element (OSE) to provide OPSEC Level II Training.

Chapter 5 OPSEC Review, Assessment and Survey

Section I. OPSEC Review

5-1. General

The OPSEC review is an evaluation of a document to ensure protection of sensitive or critical information. The document may be a memorandum, letter, message, briefing, contract, news release, technical document, proposal, plan, order, and response to Freedom of Information Act (FOIA), or Privacy Act requests or other visual or electronic media.

5-2. Procedures

a. An individual may request an OPSEC review, or the commander may direct one. Standing operating procedures will state which documents automatically go to the OPSEC officer for a review. News releases and responses to FOIA and Privacy Act requests are examples of documents suitable for automatic review.

b. The OPSEC review may take little time or require extensive research over several days. When corrective action is necessary, such as a classification review, the OPSEC officer will provide written recommendations to the appropriate official for immediate action.

c. Technical papers and reports must contain distribution statements according to AR 25-30, AR 70-11, AR 70-31, and MIL STD 1806 for contractors producing technical information for the U.S. government.

Section II. OPSEC Assessment

5-3. General

The OPSEC assessment is an analysis of an operation, activity, exercise, or support function to determine the overall OPSEC posture and to evaluate the degree of compliance of subordinate organizations with the published OPSEC plan or OPSEC program.

5-4. Procedures

a. The organization's OPSEC officer conducts the OPSEC assessment on his own initiative or as the commander directs. He submits a written assessment with results and recommendations to the commander. Contact the local CI office for multi-disciplined CI assistance.

b. Use Appendix F OPSEC Assessment as a guide to conduct an OPSEC assessment.

Section III. OPSEC Survey

5-5. General

The OPSEC survey is a method to determine if there is adequate protection of critical information during planning, preparation, execution, and post-execution phases of any operation or activity. It analyzes all associated functions to identify sources of information, what they disclose, and what can be derived from the information.

a. The objective is to identify OPSEC vulnerabilities in operations or activities, which an adversary could exploit to degrade friendly effectiveness or surprise. The survey helps the commander to monitor OPSEC measures and take further action to maintain essential secrecy.

b. The survey is resource intensive. Conduct an OPSEC assessment first and evaluate its results. Then determine if there is a serious need for an OPSEC survey.

c. The OPSEC survey checks how well a unit executes its plan to protect critical information identified in its EEFI.

(1) Use EEFI, identified in the unit's OPSEC plan, to guide the survey. This is essential, but exercise caution. The unit may not understand EEFI, so it may not have a valid list. The survey team might have to assist the unit to formulate effective EEFI.

(2) When EEFI have not been determined, the surveyed unit's commander must first establish them. Without EEFI, the team cannot determine that actual OPSEC weaknesses exist.

d. The planning, data collection, and analysis functions involved in the survey are common to any analytic effort. An effective survey requires careful prior planning, thorough data collection, and thoughtful analysis of the results. It is essential for survey team members to have experience in the functional areas they will examine. Team members should also have experience in either intelligence or general program analysis.

e. The OPSEC survey attempts to reproduce the intelligence image that a specific operation projects. (The survey differs from an adversary's collection effort, since it occurs within a limited timeframe, and normally does not use covert means.) From that image, it identifies exploitable information sources. It verifies the existence of indicators by examining all of an organization's functions during planning, coordination, and execution of the operation. The examination traces the chronological flow of information from start to finish for each function.

f. OPSEC surveys vary according to the nature of the information, the adversary collection capability, and the environment. In combat, surveys identify weaknesses, which can endanger ongoing and impending combat operations. In peacetime, surveys assist in correcting weaknesses, which disclose information useful to adversaries in future conflict.

g. An OPSEC survey is not an inspection in the traditional sense. There is no grade. A survey is not a check on the effectiveness of a command's security programs or adherence to security directives. Adherence to some security measures can provide indicators of friendly intentions. Overly stringent application of security for classified materials may actually impede operational effectiveness.

(1) To encourage open dialogue, a survey team will not attribute data to its source. An accurate survey depends on cooperation by all personnel in surveyed organizations.

(2) There is no report to the surveyed unit's higher headquarters. As appropriate, the survey team can provide lessons learned without reference to specific units or individuals.

h. There are two types of surveys.

(1) A command survey concentrates on events, which happen solely within the command. It uses the personnel resources of the command to conduct the survey.

(2) A formal survey includes supporting activities beyond the control of the operation that is the focus of the survey. (It crosses command lines with prior coordination.) The survey team includes members from inside and outside the surveyed command. A letter or message initiates the formal survey. It states the subject, team members, and dates of the survey. It can also list commands, activities, and locations.

i. Each survey is unique, as it reflects the operation or activity it analyzes. Nevertheless, there are common procedures, which subsequent paragraphs discuss. (See fig 5-1 for an outline.)

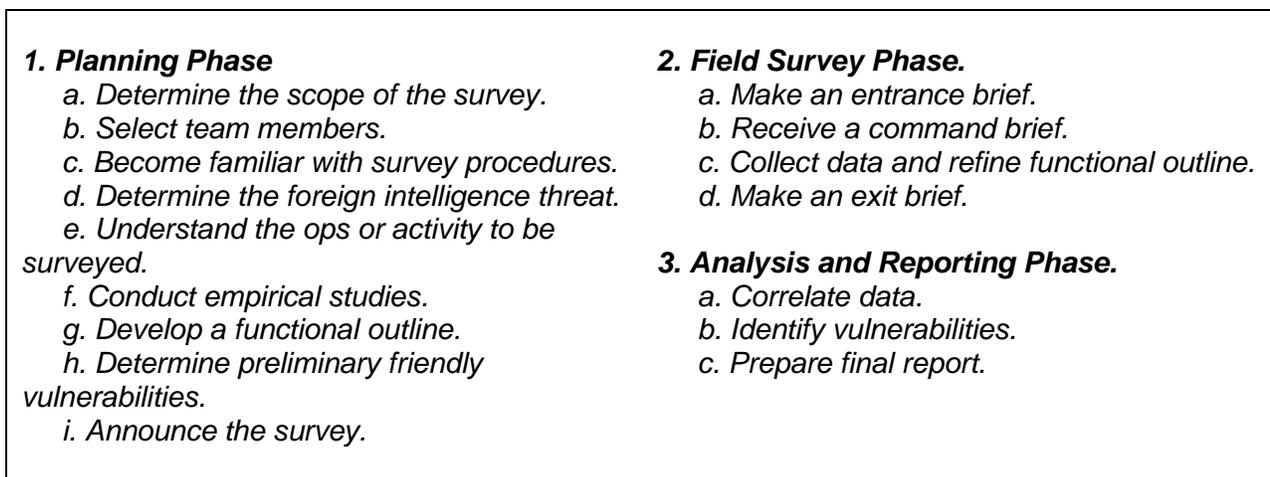


Figure 5-1. OPSEC Survey Sequence of Actions

5-6. Planning Phase

Preparation time depends on the nature and complexity of the activities to be surveyed. Allocate sufficient time for thorough document review, coordination, and preparation of functional outlines.

a. Determine the scope of the survey. Define the scope of the survey at the start of the planning phase and keep it manageable. Geography, time, units to be observed, availability of team members, and funding impose limits. Revise the scope at a later date only if significant, new information makes the additional resource investment necessary.

b. Select team members. The survey team is multidiscipline. It includes members appropriate to the subject of the survey. Choose the team leader from the operations staff of the commander responsible for the survey. Typical team members represent the functional areas of intelligence, logistics, administration, automated information systems and communications. The survey can require other specialists, such as the leader of a COMSEC monitoring team. Bring team members together early to ensure timely and thorough preparation.

c. Become familiar with survey procedures. The advantages of previous survey experience are obvious, but such personnel may not be available. Familiarize team members with survey techniques, particularly preparation of functional outlines and data collection.

d. Determine the adversary intelligence threat. Evaluate it realistically. Findings for inflated threats, when they are really minimal or nonexistent, diminish the value of the survey. The all-source threat assessment should address the following areas:

(1) Knowledge of adversary intelligence collection activities and interests pertinent to the area concerned.

(2) Possible espionage threats.

(3) Human observation threats.

(4) Open source exploitation threats.

(5) Fixed signals intelligence (SIGINT), acoustic intelligence (ACOUSINT), and radar collection capabilities.

(6) Mobile systems with technical collection capabilities (satellites, surface ships, trucks/vans, submarines, aircraft, and so on.). For each mobile system, list collection capabilities (For example, cameras, radars, SIGINT, and ACOUSINT).

e. Understand the operation or activity to be surveyed. Review OPLANs, OPORDs, standard operating procedures (SOPs), and other directives. Read the OPSEC plan (or annex) and know the EEFI. Become familiar with the mission, concept of operation, organizational structure, and command relationships. Identify organizations participating in the surveyed activity.

f. Conduct empirical studies. These simulate aspects of the adversary intelligence threat. They support findings or identify vulnerabilities, which the survey team cannot determine through interviews or by observation. Computer modeling and communications monitoring are examples. This requires external support and long lead-time.

g. Develop a functional outline. Construct the chronology of events in the surveyed activity. Describe what, when, and where events occur, and who is involved. Do this for each functional area to include administration, intelligence, operations, logistics, communications and others as appropriate. Use any appropriate format, such as narrative, tabular, or graphic. (See fig 4-2 for a generic functional outline).

(1) Continue to refine the functional outline during the field survey phase.

(2) Use functional outlines for observations and interviews. For example, group units and facilities geographically to plan the teams travel itinerary during the field survey phase.

h. Determine preliminary friendly vulnerabilities. Use the EEFI, threat, and functional outlines to look for possible vulnerabilities (para 3-5). Identify indicators, which could enable the adversary to degrade friendly effectiveness. The classified or unclassified nature of the indicator is irrelevant.

Planned Event Sequence. Build the sequence of events that are supposed to occur (who, what, when, and where). Use OPORDs, test plans, SOPS, and so on, as source documents.
Actual Event Sequence. Describe the events that actually occur.
Analysis. Determine vulnerabilities and whether they are avoidable. If avoidable, determine whether disclosure is the result of error or normal procedures.
Note: See appendix B for sample OPSEC indicators.

**Figure 5-2. Generic Functional Outline/Profile
The Completed Profile Gives A Picture Of The Functional Area:**

b. Announce the survey. The commander of the organizations to be surveyed announces it. Survey will cover the following items:

- (1) OPSEC survey purpose and scope.
- (2) List of team members and security clearances.
- (3) Requirements for briefings and orientations
- (4) General time frame of the survey.
- (5) Administrative support.
- (6) Empirical study support.

5-7. Field Survey Phase

a. Make an entrance brief. This presentation to the commander and staff of the surveyed organization is either formal or informal. It informs them what the survey will do and how it will be conducted. Cover the purpose and scope of the survey in detail.

(1) Emphasize that the survey is not an inspection, but it is an effort to enhance the ultimate effectiveness of the operation. This briefing lays the groundwork for effective work by, and cooperation with the survey team during the field survey phase.

(2) Summarize the foreign threat and vulnerability assessment developed by the team during the planning phase. Ask the commander and staff to comment on the validity of this assessment.

b. Receive a command brief. The commander and staff of the surveyed unit provide the survey team with an overview of the operation from the command's point of view. Include a tour of the command and control center where feasible. The survey team must resolve any differences between information in the command brief and that determined by the team during the planning phase.

c. Collect data and refine functional outline. Obtain data by observation of activities, document collection, and personnel interviews. Concurrent empirical studies, such as SIGSEC monitoring, also provide data. Be alert to differences between written material, the command brief, interviews, and observations. Expect conflicting data. Determine which information is correct.

(1) Observations verify the occurrence, sequence, and exact timing of events. Interviews provide additional information essential for complete understanding. Record details of how, when, and where personnel accomplish their tasks. Relate these to the planned and observed sequence of events. Obtain copies of documents, which demonstrate potential indicators or vulnerabilities.

(2) Maintain a non-attribution policy regarding sources of information. Interviews are best conducted by two team members. Record the following points:

(a) Identification and purpose of the interview.

(b) Description of the position occupied by the person being interviewed.

(c) Details of how, when, where, and exactly what tasks the individual performs. Determine what information he receives, handles, or generates, and what he does with it.

(d) Awareness of the adversary collection threat in his actions.

(3) Review the functional outline before and after interviews to ensure coverage of all pertinent points. Modify the outline to reflect new information obtained through observations and interviews. Ultimately, each functional outline becomes a profile of actual events. It becomes a chronological record of what happened, where, how, why, and who did it. The outline also has an assessment of the vulnerability of each event to the adversary intelligence threat.

(4) Be familiar with outlines used by other team members. Be alert for information that might affect the other members.

(5) Reassemble the team daily to assess progress, compare data, and coordinate the direction of the survey. This daily discussion generates new investigative directions.

(6) The duration of the field survey phase depends on the rapidity of data collection. Surveys can require thirty or more days in the field. Some factors to consider are:

(a) The proximity of data collection locations to each other.

(b) The total number of data collection points.

(c) Transportation availability.

(d) The degree of difficulty in resolving conflicting data.

(7) As data collection proceeds, tentative findings emerge. When serious, quickly inform the responsible commander to permit early corrective actions. Development of findings while still in the field ensures access to supporting data.

d. Make an exit brief. Brief the commander prior to departure from the area. Provide the major tentative findings of the OPSEC survey.

(1) Emphasize that the findings are tentative and subject to change during detailed analysis and preparation of the survey report. As it may take some time, this exit briefing is an interim basis for corrective action.

(2) Clearly state the distribution of the final report. It is directly to the commander only.

5-8. Analysis and Reporting Phase

Correlate the data from each refined functional outline and information from empirical studies into one composite operations profile. The operations profile is a complete portrait of the operation. Analyze it to identify vulnerabilities.

a. Correlate empirical data.

(1) Merge all refined functional outlines into one time-phased outline. Describe the sequence of the operation, depict how organizations interact, and trace the flow of information through communications. Portray the information in any manner that facilitates analysis.

(2) Combine empirical data with the time-phased outline to complete the operations profile. When using it, select only data relevant to the operation.

b. Identify vulnerabilities. Look at detectable actions in the operations profile from the adversary's perspective. Detection alone is not sufficient to have a vulnerability. The adversary must be able to collect, process, and react to detectable actions in sufficient time and manner to degrade friendly effectiveness. Also look for stereotyped or repetitive patterns that are early indicators of friendly intentions.

c. Prepare final report. There is no set format for the report. Include an executive summary in lengthy reports. (See fig 5-3.)

(1) Clearly explain and substantiate vulnerabilities or actual sources of detectable indicators. Address all vulnerabilities, even those impossible to eliminate or reduce. This allows the commander to realistically assess the operation.

(2) Limit the length and classification of the threat statement. It only needs to substantiate reported vulnerabilities. Include it either in the main body or as an annex. Concise parts applicable to a particular finding may precede or follow the explanation of the finding.

(3) Introduce each vulnerability with a headline. Follow with a description of the finding. This can include the piece of the operation that entails the vulnerability and the relevant threat. There are several ways to present the vulnerabilities.

(a) In order of significance.

(b) In order of occurrence.

(c) By functional area.

(4) Corrective actions are the prerogative of the surveyed command. The report includes recommendations with the findings.

I. OVERVIEW

A. *Background. Origin, purpose, scope of survey; threat/vulnerability assessment.*

B. *Conduct of Survey. Brief discussion of methodology; team composition; major units or activities visited; time-frame of survey.*

II. SUMMARY OF SIGNIFICANT FINDINGS

Extract of major findings from paragraph III below.

III. ANALYSIS, CONCLUSIONS. AND FINDINGS

A. *The body of the report. Discussions and findings may be listed chronologically, by command, or chronologically within commands.*

B. *Suggested format for each finding:*

1. *Finding.*

2. *Analysis and Discussion.*

3. *Conclusion or Recommendation.*

Figure 5-3. Example OPSEC Survey Report Format

Appendix A References

Section I. Required Publications

AR 1-201, Army Inspection Policy (Cited in para 2-1e.)

AR 380-5, Department of the Army Information Security Program (Cited in para D-2, Appendix D)

AR 380-49, Industrial Security Program

AR 380-381(U), Special Access Programs (SAPs) and Sensitive Activities

AR 381-12, Subversion and Espionage Directed Against U.S. Army (SAEDA) (Cited in para 2-12b.)

AR 530-1, Operations Security (OPSEC)

DODD 5205.02, DOD Operations Security (OPSEC) Program

DODM 5205.02, DOD Operations Security (OPSEC) Program Manual

Section II. Related Publications

A related publication is additional information. The user does not have to read it to understand this publication.

AR 25-55, The Department of the Army Freedom of Information Act Program

AR 70-14, Publication and Reprints of Articles in Professional Journals

AR 70-45, Scientific and Technical Information Program

AR 340-21, The Army Privacy Program

AR 380-40, Policy for Safeguarding and Controlling Communications Security (COMSEC) Materiel

AR 380-53, Information Systems Security Monitoring

AR 380-67, The Department of the Army Personnel Security Program

AR 381-10, U.S. Army Intelligence Activities

AR 381-20, The Army Counterintelligence Program

AR 715-30, Secure Environment Contracting

DODD 5205.7, Special Access Programs (SAP) Policy

DOD 5220.22-M, National Industrial Security Program Operating Manual

FM 3-37, Protection

Joint Pub 3-13, Information Operations

Joint Pub 3-13.3, Operations Security

CJCSI 3213.01C, Joint Operations Security

CJCSM 6231.05B, Manual for Employing Joint Tactical Communications – Joint Communications Security

**Section III
Prescribed Forms**

This section contains no entries.

**Section IV
Referenced Forms**

DD Form 254, Contract Security Classification Specification

Appendix B

OPSEC Indicators

B-1. Types

- a. Profile indicators give an analyst patterns and signatures that show how activities are normally conducted.
- b. Deviation indicators provide contrasts to normal activity, which help the adversary gain appreciations about intentions, preparations, time, and place.
- c. Tip-off indicators highlight information that otherwise might pass unnoticed. These are most significant when they warn an adversary of impending activity. This allows him to pay closer attention and to task additional collection assets.

B-2. Characteristics

View an indicator's characteristics for its usefulness to the collector on its own and when combined with other indicators. Operations security uses an adversary's perspective and modifies friendly profiles accordingly.

- a. Signature. This characteristic makes an indicator identifiable or causes it to stand out. Uniqueness and stability are properties of a signature. Uncommon or unique features reduce the ambiguity of an indicator. They minimize the number of other indicators that an adversary must observe to confirm its significance. An indicator's signature stability, which implies constant or stereotyped behavior, can allow an adversary to predict intentions. Varying the behavior decreases the signature's stability and thus increases the ambiguity of the adversary's observations. Procedural features are an important part of any indicator's signature and may provide the greatest value to an adversary. They identify how, when and where the indicator occurs and what part it plays in the overall scheme of operations and activities.
- b. Associations. These are the keys to interpretation. Compare current with past information to identify possible relationships. Continuity of actions, objects, or other indicators, which register as patterns, provides another association. Such continuity can result from repetitive practices or sequencing instead of from planned procedures. When detecting some components of symmetrically arrayed organizations, assume the existence of the rest. For example, suspect the presence of an entire infantry battalion, when intelligence detects only the headquarters company and one line company. When taken as a whole, the pattern can be a single indicator, which simplifies the adversary's problem.
- c. Profiles. There are other indicators that have not been observed or detected. Each functional activity has a profile of unique indicators, patterns, and associations. The profile of an aircraft deployment, for example, may be unique to the aircraft type or mission. This profile, in turn, has several sub profiles for the functional activities needed to deploy the particular mission aircraft (for example, fuels, avionics, munitions, communications, air traffic control, supply, personnel and transportation). If a functional profile does not change from one operation to the next, it is hard for an analyst to interpret. If, however, it is unique, it may contain the key or only indicator needed to understand the operation. Unique profiles cut the time needed to make accurate situation estimates. They are primary warning tools because they provide a background for contrasts.
- d. Contrasts. These are the most reliable means of detection because they use changes in established profiles. They are simpler to use because they only need to be recognized not

understood. One question prompts several additional ones concerning contrasts in profile. The nature of the indicator's exposure is an important aspect when seeking profile contrasts.

e. Exposure. Duration, repetition, and timing of an indicator's exposure affect its importance and meaning. Limited duration and repetition reduces detailed observation and associations. An indicator that appears over a long period of time becomes part of a profile. An indicator that appears for a short time will likely fade in to the background of insignificant anomalies.

B-3. Sample OPSEC Indicators

The following paragraphs provide a few examples of OPSEC indicators. There are many other indicators possible for the wide range of Army operations and activities. The purpose of this appendix is to stimulate thinking. Do not use it as a checklist, since each operation or activity will have indicators unique to itself.

B-4. Administration

- a. Temporary duty (TDY) orders.
- b. Conferences.
- c. Transportation arrangements
- d. Billeting arrangements.
- e. Medical care.
- f. Schedules.
- g. Plans of the day.
- h. Notice to airmen (NOTAM) and International Civil Aviation Organization (ICAO) notices.
- i. Reserve mobilization.
- j. Change of mail addressees or arrangements to forward mail on a large scale.
- k. Runs on post exchange for personal articles.
- l. Emergency personnel requisitions and fills for critical skills.
- m. Emergency recall of personnel on leave and pass.
- n. Leave for large groups or entire units.
- o. Changes to daily schedules.

B-5. Operations, Plans, and Training

- a. Changes in defense readiness condition (DEFCON).
- b. Movement of forces into position for operations.
- c. Abnormal dispersions or concentrations of forces.
- d. Deviations from routine training.
- e. Rehearsals and drills for a particular mission.
- f. Exercises and training in particular areas with particular forces.
- g. Standard reactions to hostile acts.
- h. Standard maneuvers or procedures.
- i. Standard force mixes and numbers to execute particular missions.
- j. Changing guards at fixed times.
- k. Appearance of special purpose units (bridge companies, path- finders, and so on.).
- l. Change in task organization or arrival of new attachments.
- m. Artillery registration in new objective area.
- n. Surge in fast food (that is, pizza) deliveries to planning staffs at major headquarters.
- o. Unit and equipment departures from normal bases.
- p. Fixed schedules and routes.

B-6. Communications

- a. Telephone calls among participants in an Operation.
- b. Establishment of command nets.
- c. Changes in message volume, such as increased radio, teletype, and telephone traffic.
- d. Units reporting to new commanders.
- e. Identification of units, tasks, or locations in unsecured transmissions
- f. Increased communications checks.
- g. Unnecessary or abnormal reporting.
- h. Sudden imposition of COMSEC measures, such as radio silence.
- i. Appearance of new net control stations.
- j. Communications exercises.
- k. Appearance of different cryptographic equipment or materials.

B-7. Intelligence, Counterintelligence, and Security

- a. Concentrated reconnaissance in a particular area.
- b. Embarking or moving special equipment.
- c. Recruitment of personnel with particular language skills.
- d. Routes of reconnaissance vehicles.
- e. Sensor drops in target area.
- f. Increased activity of friendly agent nets.
- g. Trash that contains unit data.
- h. Increased ground patrols.
- i. Unusual or increased requests for meteorological or oceanographic information.
- j. Unique or highly visible security to load or guard special munitions or equipment.
- k. Adversary radar, sonar, or visual detection's of friendly units.
- l. Friendly unit identifications through COMSEC violation, physical observation of unit symbols, and so forth.

B-8. Logistics

- a. Volume and priority of requisitions.
- b. Package or container labels that show the name of an operation, program, or unit designation.
- c. Pre-positioning equipment or supplies.
- d. Procedural disparities in requisitioning and handling.
- e. Accelerated maintenance of weapons and vehicles.
- f. Presence of technical representatives.
- g. Unusual equipment modification.
- h. Increased motor pool activities.
- i. Test-equipment turnover.
- j. Special equipment issue.
- k. POL and ammunition stockpiling.
- l. Upgraded lines of communication (LOCS).
- m. Delivery of special or uncommon munitions.
- n. New support contracts or host nation agreements.
- o. Arranging for tugs and harbor pilots.
- p. Requisitions in unusual quantities to be filled by a particular date.

B-9. Engineer

- a. New facility leases.
- b. Construction of mock-ups for special training.
- c. Production of unusual numbers of maps and charts for specific locations.

B-10. Medical

- a. Movement of deployable medical sets (DEPMEDS).
- b. Stockpiling plasma and medical supplies.

B-11. Emissions Other Than Communications

- a. Radar and NAVAIDS that reveal location or identity.
- b. Normal lighting in a blackout area.
- c. Operating at high speed in water.
- d. Loud vehicle or personnel movements.
- e. Smoke and other odors.

Appendix C

Sample Questions for EEFI

C-1. Courses of Action (COAS)

- a. What specific COAs are U.S. and allied commands planning?
- b. What possible COAs are Civilian and Non-Governmental Organizations (NGO) planning?

C-2. Forces

- a. What U.S. and allied combat forces are earmarked for possible COAs?
- b. What are their levels of readiness?
- c. Where are they located?

C-3. Command, Control and Communications

- a. What are U.S. and allied command arrangements for executing COAs?
- b. Where will commanders and command posts be located?
- c. What are command post vulnerabilities to attack?
- d. What are the communications capabilities available for the commander to control and coordinate assigned forces?
- e. Where are dedicated communications sites located?

C-4. Logistics

- a. What is the logistical posture of U.S. and allied forces?
- b. How quickly can ground and air forces be deployed and redeployed?
- c. What are the pertinent ground, air, and sea LOCs, and what are the locations of storage depots, ports, and airfields?
- d. What are the vulnerabilities to interdiction of the LOCs?

C-5. Supplies

- a. What levels of supplies are available to support combat forces immediately?
- b. Where are pre-positioned supplies?
- c. How long can combat be sustained with those supplies?

C-6. Locations

- a. When will exercises and operations occur?
- b. Where are participating forces located?

C-7. Vulnerabilities

- a. What are the defensive dispositions?
- b. What sensors and other capabilities are available to detect attacks?
- c. What vulnerabilities to attack exist?

C-8. Intelligence

- a. What are the intelligence, surveillance, and reconnaissance resources available to support the commander?
- b. Where are those capabilities located?
- c. What operations are being conducted and what are their apparent goals?
- d. How can these capabilities be exploited or destroyed?

C-9. Rules of Engagement (ROE)

- a. What are the policies and ROE that govern the use of weapons and electronic or acoustic warfare systems?
- b. Is the ROE clearly understood by all levels and soldiers?

C-10. Allies

- a. Which nations will provide support to the U.S.?
- b. What vulnerabilities exist that could be exploited to reduce or eliminate such support?

C-11. Maintenance

- a. What are the maintenance and salvage capabilities of U.S. and allied forces?
- b. To what degree can these capabilities support and sustain forces in combat?
- c. What are their vulnerabilities to attack?

C-12. Weapons

- a. What are the characteristics and capabilities of weapons and electronic systems available to U.S. and allied forces?
- b. What are the doctrines for using various weapons?
- c. What are the indicators that nuclear weapons will be employed?

C-13. Psychological Operations (PSYOP)

- a. What are intended psychological warfare and subversion operations?
- b. What are the plans to exploit vulnerabilities?
- c. What operations are underway?
- d. What are the vulnerabilities of U.S. forces to psychological warfare and subversion?

C-14. Unconventional Warfare

- a. What are intended sabotage and direct action mission targets?
- b. What vulnerabilities are planned for exploitation?
- c. What capabilities exist to conduct such operations?
- d. What U.S. agencies control the resources involved?

C-15. Deception

- a. What political and military deceptions are planned?
- b. What operations are underway?
- c. What U.S. agencies are conducting operations?
- d. What are the vulnerabilities of U.S. commanders and staffs to deception?
- e. What are the vulnerabilities of U.S. and allied forces to political deception?

C-16. Counterintelligence

What are U.S. counterintelligence capabilities to detect and neutralize espionage and sabotage nets?

C-17. Medical

- a. What are our casualty figures, both actual and projected?
- b. Which VIPs are being treated by our Medical Treatment Facilities (MTF)?
- c. What is our overall bed/treatment capacity?
- d. What increased medical supplies (that is, vaccines, blood products, and so forth) are required by unit or theater?

C-19. Special Access Programs

- a. What organizations and contractors are involved in the SAP?
- b. What is the mission or subject of the SAP?
- c. How long will the SAP be operational? What is the current stage of development of the SAP?
- d. What are the security procedures for the SAP?
- e. What is the budget for the SAP?

C-20. Automated Information Systems (AIS)

- a. What measures are taken to prevent unauthorized access to AIS's?
- b. Are AIS's approved/certified to process unclassified-sensitive information?
- c. Is AIS hardware equipment protected within an office environment and/or remote site?

Appendix D

OPSEC Relations to Other Programs

D-1. Background

The U.S. Army has a long history of successful operation's security from the Revolutionary War's Yorktown campaign to OPERATION DESERT STORM. Current OPSEC methodology originated during the Vietnam War. The Purple Dragon Team under U.S. Pacific Command, viewed friendly combat operations from the enemy's perspective. The team used systems analysis to determine what critical information the enemy could learn about friendly operations. The following paragraphs address OPSEC relationships to other programs.

D-2. Information Protection

AR 380-5 provides guidance for classifying material. Protective measures deny unauthorized personnel access to classified material. Both the threat of open source exploitation and procedures intended to keep classified material from appearing in open sources are OPSEC concerns. Bits of information conveyed in non-secure radio transmissions, public releases, briefings for the public, friendly conversations, telephone calls, and so forth, permit hostile intelligence analysts to piece together U.S. intentions and military capabilities. OPSEC prevents critical information (some of which is classified) from appearing in open sources.

D-3. Communications Security (COMSEC)

COMSEC is of particular concern to OPSEC. The intercept of non-secure communications is a significant source of intelligence information for adversaries. Components of COMSEC are cryptographic, transmission, and emissions security.

a. Cryptographic security is classified information transmitted by message or telephone, which is encrypted or sent using an authorized code. OPSEC is concerned with any deviation from established practices that would permit any adversary to "read" U.S. message traffic.

b. Transmission security has a major interface between OPSEC and COMSEC. Transmission security is concerned with the conclusions that can be determined from the externals to communications signals, the intercept of a signal (such as, deviation of location or identity), and the patterns and volumes of communications.

c. Emission security (for example, TEMPEST) is concerned with identifying and eliminating unintentional radiation that conveys classified information.

D-4. Electronic Security (ELSEC)

ELSEC is concerned with denying adversaries the information derived from interception and study of non-communications electromagnetic emissions. One part of ELSEC similar to transmission security involves controlling the emissions of radars, navigational aids, and weapons emitters to deny intercepts. Another pan involves reducing the information content of the emitters to make them more difficult to identify and locate.

D-5. Physical Security

Physical security consists of protective measures to deny unauthorized personnel access to specific areas, facilities, material, or classified information. The implementation of protective measures can reveal vulnerabilities (for example, combat patrolling at predictable intervals, personnel routinely and predictably leaving a facility unattended, easily seen sensors, changing military police patrols at set times, reacting predictably to alarms, and being careless or lazy in implementing physical security measures). Physical security can be an OPSEC measure.

D-6. Emission Control (EMCON)

EMCON encompasses controlling all radiation that hostile sensors can detect. A key purpose of EMCON is to prevent detection or identification. EMCON thus crosses the boundaries of OPSEC, COMSEC, ELSEC, and EW.

D-7. Military Deception (MD)

MD supports military operations through the application of techniques that simultaneously deny true information or indicators and convey or display false information to adversaries. MD actions mislead adversaries, causing them to derive and accept desired appreciations of U.S. military capabilities, intentions, operations, and other activities. Depending on the objective, MD can be an OPSEC measure, or OPSEC can support MD. When procedural or physical security means are unavailable for controlling OPSEC vulnerabilities, MD can mislead adversaries, thereby minimizing the OPSEC vulnerability.

D-8. Force Protection

Force protection consists of active and passive measures to deter threats directed toward soldiers, their family members, civilians, and the facilities and equipment that support them. Force Protection uses the planned, integrated, and synchronized application of operations security, combating terrorism, physical security, base defense, personal protective services, law enforcement, and crime prevention. Counterintelligence supports force protection, providing threat information and indicators.

D-9. Computer Security (COMPUSEC)

COMPUSEC prevents the intentional or accidental penetration of Automated Information Systems (AIS). It avoids the disclosure, modification, or destruction of AIS and associated data. Examples are "hacker" penetrations and computer "virus attacks"

D-10. Program Protection Planning (PPP)

The DoD Acquisition Systems Protection Master Plan, dated 12 May 1992, provides a coherent strategy to protect defense technology. It requires PPP for acquisition systems. The PPP uses security disciplines and OPSEC to achieve protection.

Appendix E

The Threat

E-1. Summary

The intelligence threat consists of multiple and overlapping collection efforts targeted against all sources of Army information. Potential adversaries devote significant resources to monitor U.S. military operations and activities on a daily basis. The threat can produce reliable information on the U.S. military establishment and our capabilities, intentions, and vulnerabilities in direct relation to the degree that he is able to collect meaningful information of intelligence value. The threat is also shifting the emphasis in targeting. Foreign targeting of American technology is increasing for economic as well as military reasons. Technology transfer will continue to remain a major concern in the future. The major threat collection disciplines fall in four areas:

- a. Human Intelligence (HUMINT).
- b. Imagery Intelligence (IMINT).
- c. Signals Intelligence (SIGINT).
- d. Measurement and Signature Intelligence (MASINT).

E-2. Human Intelligence Threat

a. The multidiscipline approach to intelligence collection includes the use of human sources to gain access to information not accessible to other collection assets. HUMINT employs overt, covert, and clandestine operations to achieve worldwide collection objectives.

b. Overt collection operations gather intelligence information from open sources. Vast amounts of information of great interest to foreign intelligence services are readily available. Open sources include newspapers, magazine advertisements; government and trade publications, contract specifications, congressional hearings, computers, and other public media. In excess of 75 percent of the threat's intelligence needs can be satisfied through access to open sources without risk and at minimum cost. Threat HUMINT collectors include official diplomatic and trade representatives, visitors, exchange students, journalists, and military personnel legitimately in the United States.

c. Clandestine collection activities are pursued under cover of business or other activities. Attempts may be made to buy material through third parties or directly as a commercial transaction. Agents may pose as scientists in international projects or symposia, as insurance agents to learn details of a ship's cargo, or as research groups to join international computer nets to obtain data.

d. Clandestine collection operations encompass those activities conducted illegally in a manner intended to assure operational secrecy while providing plausible denial for the sponsoring government. These operations target human sources for information not available through open sources.

(1) Clandestine operations are usually expensive and time consuming. They also involve potential embarrassment to the sponsoring government upon discovery. Therefore, the value of the desired information must justify the costs and risks involved.

(2) Greed, financial gain, alcoholism, drug abuse, sexual perversion, marital infidelity, and financial indebtedness are among the human failures exploited by threat HUMINT collectors. Disenchanted idealists are also a fertile source of information.

(3) Another recruitment technique involves misrepresentation of status or the “false flag” approach. A threat agent will attempt to pass himself off as an agent of a U.S. agency or of a friendly government to solicit cooperation.

E-3. Imagery Intelligence Threat

Adversaries can obtain IMINT from land, sea, air, and space platforms. The most serious threat at the strategic level stems from photo-reconnaissance and open skies observation flights. At the tactical level, airborne collection possesses the greatest IMINT threat. From a commercial perspective, the adversary is capable of obtaining open source imagery that provides a one meter resolution for a minimal fee and a short turnaround time. The constant improvement of technical equipment and the employment of combinations of sensors enhance the quality and timeliness of the intelligence product for our adversaries.

E-4. Signals Intelligence Threat

SIGINT incorporates communications intelligence (COMINT) electronics intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT).

a. COMINT has the greatest impact on the day-to-day performance of Army missions. It derives information from the study of intercepted electromagnetic communications. Prime sources of valuable COMINT include clear voice or non-encrypted telephone and radio communications. Major adversaries use various intercept platforms and have a worldwide COMINT capability.

b. ELINT is technical or intelligence information derived from non-communications electromagnetic radiations, such as that emitted by radar.

c. FISINT is derived from the intercept and analysis of electronically transmitted data containing measured parameters of performance, either human or mechanical. Examples are transmitted data on an astronaut’s bio functions or of a ballistic missiles performance.

E-5. Measurement and Signature Intelligence Threat

MASINT is scientific and technical intelligence obtained by quantitative and qualitative analysis of data derived from technical for the purpose of identifying any distinctive features associated with the source, emitter, or sender and to facilitate subsequent identification or measurement. The eight primary disciplines of MASINT are infrared, seismic, radar, laser, effluent, nuclear, optical and unintentional radiation. MASINT includes all technical intelligence except SIGINT and overhead imagery.

**Appendix F
OPSEC Assessment**

OPSEC PROGRAM SELF-INSPECTION CHECKLIST

Answer yes, no, or not applicable (NA) to each of the items on the checklist. Certain items are repeated with slight variation as you move to the next tier. Each tier assumes the requirements of the previous tier(s) have been accomplished and are maintained.

1. Tier One OPSEC Programs. NOTE: If all items are answered "yes", go on to Tier Two.			
ITEM	YES	NO	NA
1.1. Has an OPSEC Program Manager been appointed?			
1.1.1. Is there an appointment letter?			
1.1.2. Has the appointment been announced?			
1.2. Does the OPSEC Program Manager dedicate between 10% and 30% of available duty hours to OPSEC?			
1.3. Has the [commander/director] signed a local policy letter?			
1.3.1. Has the letter been distributed to all managers/supervisors?			
1.3.2. Are all personnel aware of the policy?			
1.3.3. Is the policy periodically reviewed and updated as necessary?			
1.4. Has the [commander/director] appointed an OPSEC Working Group?			
1.4.1. Does the Working Group meet periodically?			
1.4.2. Is the role of the Working Group clearly defined?			
1.4.3. Have all Working Group members been trained?			
1.4.4. Are Working Group members who leave the organization replaced?			
1.4.5. Is there a mechanism in place to train new Working Group members?			
1.5. Has a Critical Information list (CIL) been published?			
1.5.1. Has the CIL been approved by the [commander/director]?			
1.6. Does the organization have an awareness training program?			
1.6.1. Are all newly assigned personnel trained within 90 days of assignment?			
1.6.2. Do all personnel receive awareness training at least annually?			

NOTES:

2. Tier Two Programs. NOTE: If all items are answered "yes", go on to Tier Three.			
ITEM	YES	NO	NA
2.1. Does the Program Manager dedicate 30% to 50% of available duty hours to OPSEC?			
2.2. Does the Working Group meet quarterly?			
2.3. Have all Working Group members been trained?			
2.4. Are Working Group members who leave the organization replaced?			
2.5. Is there a mechanism in place to train new Working Group members?			
2.6. Are all newly assigned personnel trained within 60 days of assignment?			
2.6.1. Has the [commander/director] established frequency requirements for unit personnel awareness training?			
2.7. Has the OPSEC Program Manager prepared a unit OPSEC plan?			
2.7.1. Is the plan signed by the [commander/director]?			
2.7.2. Has the plan been distributed to all managers/supervisors?			
2.8. Does the Program Manager keep a continuity [file/book]?			
2.9. Is senior leadership actively involved in the OPSEC program?			
2.9.1. Participates in awareness training?			
2.9.2. Addresses OPSEC issues in all-hands meetings?			
2.9.3. Regularly includes OPSEC concerns in senior staff meetings?			
2.9.4. Requires OPSEC input to planning and special events?			
2.10. Have coordinators been assigned in accordance with local policy?			
2.10.1. Does the Program Manager meet regularly with coordinators?			
2.10.2. Is the role of the coordinator clearly defined?			
2.10.3. Have all coordinators been trained?			
2.10.4. Are coordinators who leave the organization replaced?			
2.10.5. Is there a mechanism in place to train new coordinators?			
2.11. Does the Program Manager have a plan to use end-of-year money?			
2.12. Is a survey or assessment conducted at least once annually?			
2.13. Has the Program Manager developed a support network to include:			
2.13.1. Counterintelligence specialists?			
2.13.2. Appropriate security specialists, such as IT and communications security?			
2.13.3. Threat analysis experts?			
2.13.4. Other OPSEC experts?			

NOTES:

3. Tier Three Programs			
ITEM	YES	NO	NA
3.1. Does the Program Manager dedicate 70% to 100% of available duty hours to OPSEC?			
3.2. Are all newly assigned personnel trained within 30 days of assignment?			
3.3. Do all personnel receive awareness training at least quarterly?			
3.4. Does the Program Manager document all organizational OPSEC training?			
3.5. Does the Program Manager contribute to the local [newspaper/newsletter]?			
3.5.1. Are copies maintained with the OPSEC program records?			
3.6. Does the Program Manager conduct self-inspections quarterly?			
3.7. Is a survey or assessment conducted at least once annually?			
3.7.1. Are countermeasures implemented to correct vulnerabilities?			
3.8. Is OPSEC incorporated in local exercises?			
3.9. Is the Program Manager part of the emergency action team?			
3.10. Does the commander require OPSEC support for [contingencies/emergencies]?			
3.11. Is OPSEC incorporated into standing operations plans?			
3.12. Does the [commander/director] have written policies on the use of secure communications?			
3.13. Does the Program Manager have input to web content management?			
3.14. Does the [commander/director] request COMSEC monitoring at least once annually?			
3.15. Does the OPSEC program have a budget for training and awareness materials?			

NOTES:

**Appendix G
Operations Security CIP Checklist**

STAFF ELEMENT: G3
SUB-FUNCTION: Operations Security (OPSEC)

<u>INSPECTION ITEM AND REFERENCE</u>	<u>COMPLY</u>	<u>NON-COMPLY</u>	<u>N/A</u>
References:			
a. AR 530-1, Operations Security (OPSEC)	___	___	___
b. AK Reg 530 –1, Operations Security (OPSEC)	___	___	___
c. Respective MSC/Installation OPSEC Program	___	___	___
1. Has the unit developed and implemented an OPSEC Program? (AK Reg 530-1)	___	___	___
2. Does unit's OPSEC Program comply with minimal requirements established in AK Reg 530-1?	___	___	___
a. Commander has designated an OPSEC Officer in writing.	___	___	___
b. Established an OPSEC plan and/or SOP.	___	___	___
c. Established a viable and comprehensive OPSEC training program.	___	___	___
d. Established requirements for annual review of OPSEC procedures.	___	___	___
e. Provided guidance and assistance to subordinate organizations during preparations of operations, contingency and exercise plans.	___	___	___
(NOTE: Any "No" results in "No" for item #2.)			
3. Are OPSEC Annexes/Appendices/Tabs to OPLAN/OPORDs routinely developed in preparation for all operations, exercises, and activities? (AK Reg 530-1, para 8g(4))	___	___	___
4. Is the unit OPSEC Officer familiar with the 5-step OPSEC process? (AR 530-1, Chapter 3, para 3-2 b. (1) (a) – (e))	___	___	___
5. Do all newly assigned personnel receive OPSEC initial training within 30 days of arrival? (AK Reg 530-1, para 4-2a(1))	___	___	___
6. Do assigned personnel received annual OPSEC Awareness Training? (AK Reg 530-1 Appendix H)	___	___	___
7. Did the unit prepare and submit an annual OPSEC Report for the previous FY? (AR 530-1, Chapter 2, Appendices H and I)	___	___	___

	<u>COMPLY</u>	<u>NON-COMPLY</u>	<u>N/A</u>
8. Does MSC review subordinate units' compliance with unit OPSEC program through MSC CIP? (AR 530-1, Chapter 5 para 5-4 c., Appendix H, para H-3)	—	—	—
9. Has OPSEC Survey or Assessment been conducted by unit during past FY? (AR 530-1 Chapter 5; AK Reg 530-1, Chapter 5)	—	—	—
10. Is MSC OPSEC Officer aware of names of subordinate units OPSEC Officers?	—	—	—
11. Is EEFI widely disseminated amongst subordinates? (AR 530-1, Chapter 5, para 5-4)	—	—	—
12. Is the MSC actively attempting to heighten sensitivity to OPSEC? (Posters, articles, Web pages, etc.)	—	—	—

Unit Inspected: _____

Unit OPSEC Officer Name: _____

Primary Inspector Sign and Date: _____

Appendix H

OPSEC Working Group (OWG)

OPSEC Officers of designated staff agencies provide/oversee program for their staff section. Additionally, the officers serve as members of the OWG. Other offices should appoint an OPSEC Officer, and may attend OWG if they desire.

- a. OSD-PER (G1)
- b. OID (G2)
- c. OMD (G3/5/7)
- d. OSD-LOG (G4)
- e. OCCD (G6)
- f. CMO (G9)
- g. OFD
- h. OPD
- i. PAO
- j. IG
- k. Surgeon
- l. Engineers
- m. SJA
- n. Chaplain
- o. Secretary General Staff
- p. STB-K

Glossary

Section I. Abbreviations

ACOUSINT	Acoustical Intelligence
AMC	Army Material Command
ARTEP	Army Training and Evaluation Program
CDRL	Contract Data Requirements List
CI	Counterintelligence
CJCS	Chairman, Joint Chiefs of Staff
CMO	Civil Military Operations
COA	Course of Action
COMINT	Communications Intelligence
COMSEC	Communications Security
C2	Command and Control
C4I	Command and Control Warfare
C4	Command, Control, Communications and Computers
DA	Department of the Army
DCSINT	Deputy Chief of Staff for Intelligence
DCSOPS	Deputy Chief of Staff for Operations and Plans -
DCSPER	Deputy Chief of Staff for Personnel
DEFCON	Defense condition
DOD	Department of Defense
EAC	Echelons above Corps
EEFI	Essential Elements of Friendly Information
EI	Essential Elements Of Information
ELINT	Electronic Intelligence
ELSEC	Electronic Security

EMCON	Emission Control
EW	Electronic Warfare
FISINT	Foreign Instrumentation Signals Intelligence
FM	Field Manual
FIS	Foreign Intelligence Service
FOIA	Freedom of Information Act
HQDA	Headquarters, Department of the Army
HUMINT	Human Intelligence
IMINT	Imagery Intelligence
INSCOM	U.S. Army Intelligence and Security Command
ISS	Information Systems Security
JCS	Joint Chiefs of Staff
LOC	Lines of Communication
MACOM	Major Army Command
MASINT	Measurement and Signature Intelligence'
MD	Military Deception
MED	Manipulative Electronic Deception
MOP	Memorandum of Policy
MTOE	Modified Table of Organization and Equipment
NCS	Net Control Station
NOTAM	Notice to Airmen
ODCSINT	Office of The Deputy Chief Of Staff For Intelligence
OCCD	Operational Command and Control Directorate
OFD	Operational Fires Directorate
OID	Operational Intelligence Directorate

OMD	Operational Maneuver Directorate
OPD	Operational Protection Directorate
OSD	Operational Sustainment Directorate
OPLAN	Operation Plan
OPORD	Operation Order
OPSEC	Operations Security
PAO	Public Affairs Office or Officer
PM	Program Manager/Project Manager/Product Manager
POC	Point of Contact
PSYOP	Psychological Operations
RDT&E	Research, Development, Test and Evaluation
ROE	Rules of Engagement
SAP	Special Access Program
SCG	Security Classification Guide
SCI	Sensitive Compartmented Information
SIGINT	Signals Intelligence
SIGSEC	Signals Security
SOI	Signals Operating Instructions
SOP	Standard Operating Procedure
SSG	Staff Sergeant
TDA	Table of Distribution and Allowances
TDY	Temporary Duty
TRADOC	U.S. Army Training And Doctrine Command
UA	User Agency
USAF	U.S. Air Force
USAISC	U.S. Army Information Systems Command

Section II. Terms

Adversary

Individuals, organizations, or countries that must be denied critical information in order to preserve mission integrity and maintain friendly mission effectiveness and the element of surprise. Adversary, in this context, includes any individual, organization, or country with which specific information should not be shared to preserve mission integrity or the element of surprise.

Appreciations

Personal conclusions, official estimates and assumptions about another party's intentions, military capabilities and activities used in planning and decision-making.

Classified military information

Information originated by or for the DOD or its agencies or under their jurisdiction or control that requires protections in the interest of national security. It is designated TOP SECRET, SECRET, or CONFIDENTIAL as described in Executive Order 12958 or subsequent order. Classified military information may be in oral, visual, documentary, or materiel form.

Communications security (COMSEC)

Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications.

Computer security (COMPUSEC)

Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer.

Controlled Unclassified Information (CUI)

Unclassified information to which access or distribution limitations have been applied according to national laws, policies, and regulations of the United States Government (U.S. Government). It includes U.S. information that is determined to be exempt from public disclosure according to DODD 5230.25, DODD 5400.7, AR 25-55, AR 340-21, AR 530-1, and so on, or that is subject to export controls according to the International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations (EAR).

Counterintelligence (CI)

Those activities which are concerned with identifying and counteracting the threat to security posed by foreign intelligence services or organizations, or by individuals engaged in espionage, sabotage, subversion or terrorism.

Cover

Actions used to conceal actual friendly intentions, capabilities, operations and other activities by providing a plausible, yet erroneous, explanation of the observable.

Critical Information

Critical information is defined as information important to the successful achievement of U.S. objectives and missions, or which may be of use to an adversary of the United States. Critical information consists of specific facts about friendly capabilities, activities, limitations (includes vulnerabilities), and intentions needed by adversaries for them to plan and act effectively so as to degrade friendly mission accomplishment. Critical information is information that is vital to a mission that if an adversary obtains it, correctly analyzes it, and acts upon it will prevent or seriously degrade mission success. Critical information can be classified information or unclassified information.

Critical information can also be an action that provides an indicator of value to an adversary and places a friendly activity or operation at risk. The term “critical information” has superseded the term “Essential Elements of Friendly Information” (EEFI) as used in FM 3-13, EEFI now refers to critical information phrased in the form of a question in order protect classified and sensitive information.

Critical Information List (CIL)

The CIL is a consolidated list of a unit or organization’s critical information. The CIL will be classified if any one of the items of critical information is classified. The method to ensure the widest dissemination of a unit or organization’s critical information is to convert it to Essential Elements of Friendly Information (EEFI). EEFI is critical information phrased in the form of a question that does not reveal the details of critical information in order to prevent disclosure of classified and sensitive information.

Critical Program Information (CPI)

Information, technologies, or systems that, if compromised, would degrade combat effectiveness, shorten the expected combat-effective life of the system, or significantly alter program direction. This includes classified military information or controlled unclassified information (CUI) about such programs, technologies, or systems. CPI is a form of critical information specific to acquisition programs.

Electronic Security (ELSEC)

The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of non-communications electromagnetic radiations, for example, radar.

Essential Elements of Friendly Information (EEFI)

The EEFI is critical information phrased in the form of a question that does not reveal the details of critical information in order to prevent disclosure of classified and sensitive information. EEFI are phrased as questions that the adversary is likely to ask about friendly capabilities, activities, limitations, and intentions. The use of EEFI is an effective way to ensure the widest dissemination of a unit or organization’s critical information while protecting classified and sensitive information. “Critical information” supersedes the term “Essential Elements of Friendly Information” (EEFI) as used in FM 3-13. DOD and the Service Components are now using the term “critical information” for the purpose of standardization. The Army will continue to use the term EEFI in modified purpose related to critical information as previously described.

Essential Secrecy

The condition achieved from the denial of critical information to adversaries.

Field Test

Any test, demonstration, Advanced Concepts Technologies Demonstration reports, operations employment of equipment, personnel or exercise conducted at military installations, contractor facilities or on public or private domain indoors or outdoors.

For Official Use Only (FOUO)

A designation that is applied to unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA).

Force Protection

A security program consisting of actions taken to prevent or mitigate hostile actions against all DA personnel (Soldiers, DA civilians, DOD contractors, and family members), resources, facilities, and

critical information. Force protection does not include actions to defeat the adversary or protect against accidents, weather, or disease.

Friendly

Individuals, groups, or organizations involved in the specific operation or activity who have a need to know.

Government Contracting Agency (GCA)

A Government Contracting Agency is an element of a federal department or agency that is designated by the agency head and is delegated broad authority regarding acquisition functions.

Indicators

Data derived from open sources or from detectable actions that adversaries can piece together or interpret to reach personal conclusions or official estimates concerning friendly intentions, capabilities or activities.

Information Assurance (IA)

The protection of systems and information in storage, processing, or transit from unauthorized access or modifications; denial of service to unauthorized users; or the provision of service to authorized users. It also includes those measures necessary to detect, document, and counter such threats. IA encompasses communications security (COMSEC), computer security (COMPUSEC), and control of compromising emanations.

Information Operations (IO)

Information operations is the employment of the core capabilities of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified and related capabilities, to affect or defend information and information systems, and to influence decision making.

Information Security (INFOSEC)

INFOSEC is the system of policies, procedures, and requirements established under the authority of Executive Order (EO) 12958 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

Information system (IS)

Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and that includes computer software, firmware, and hardware. Included are computers, word processing systems, networks, or other electronic information handling systems and associated equipment.

Information Superiority

The degree of dominance in the information domain which permits the conduct of operations without effective opposition.

Intelligence

The product resulting from collection, processing, integration, analysis, evaluation and interpretation of available information concerning foreign areas, operations or activities.

Intelligence System

Any formal or informal system to manage data gathering, to obtain and process the data, to interpret the data and to provide reasoned judgments to decision makers on a basis for action. The term is not limited to intelligence organizations or services but includes any system, in all its parts, that accomplishes the listed tasks.

Internet

The global collaboration of data networks that are connected to each other, using common protocols to provide instant access to the information from other computers around the world.

Military Deception

Actions executed to mislead foreign decision makers, causing them to derive and accept desired appreciations of military capabilities, intentions, operations or other activities that evoke foreign actions that contribute to the originator's objectives.

Multidiscipline Counterintelligence Analysis

The process of determining the presence and nature of the total all-source adversary intelligence threat to a given target in order to provide a basis for countering or degrading the threat.

Observables

Actions that convey indicators exploitable by adversaries but that must be carried out regardless, to plan, prepare for and execute activities.

Operations Security

Operations security (OPSEC) is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

- a. Identify those actions that can be observed by adversary intelligence systems;
- b. Determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and
- c. Select and execute measure that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

OPSEC Compromise

The disclosure of critical information or sensitive information which has been identified by the Command and any higher headquarters that jeopardizes the unit's ability to execute its mission or to adequately protect its personnel and/ or equipment.

OPSEC measures

Methods and means used to gain and maintain essential secrecy about critical information. The following categories apply:

- a. Action control. The objective is to eliminate indicators or the vulnerability of actions to exploitation by adversary intelligence systems. Select what actions to undertake; decide whether or not to execute actions and determine the "who", "when", "where" and "how" for actions necessary to accomplish tasks.
- b. Countermeasures. The objective is to disrupt effective adversary information gathering or prevent their recognition of indicators when collected materials are processed. Use diversions, camouflage, concealment, jamming, threats, police powers and force against adversary information gathering and processing capabilities.

c. Counter-analysis. The objective is to prevent accurate interpretations of indicators during adversary analysis of collected materials. This is done by confusing the adversary analyst through deception techniques such as covers.

OPSEC planning guidance

Guidance that serves as the blueprint for OPSEC planning by functional elements throughout the organization. It defines the critical information that requires protection from adversary appreciations, taking into account friendly and adversary goals, estimated key adversary questions, probable adversary knowledge, desirable and harmful adversary appreciations and pertinent intelligence systems threats. It also should outline tentative OPSEC measures to ensure essential secrecy. This is also forms the contents of an OPSEC estimate.

OPSEC vulnerability

A condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision-making.

Psychological operations

Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning and ultimately the behavior of foreign governments, organizations, groups and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called PSYOP.

Publicly accessible web site

An Army web site with access unrestricted by password or Public Key Infrastructure user authorization. "Public" refers to the at-large audience on the Internet; anyone who can access a web site through a browser. (AR 25-1)

Red Team

An independent and focused threat-based effort by an interdisciplinary, simulated adversary to expose and exploit vulnerabilities in order to improve the security posture of a unit or organization to include its personnel, equipment and information systems. Red team methods, also known as red teaming, can reveal the limitations and vulnerabilities of an OPSEC program. Red teaming operations from an adversary's perspective accompanied by innovative and unconventional thinking and can be effective in revealing limitations and weaknesses that are not obvious or apparent to a unit or organization.

Requiring activity (RA)

An organization that has a requirement for goods and/or services and requests the initiation of, and provides funding for, an assisted or directed acquisition to fulfill that requirement.

Security manager

A properly cleared individual having professional security credentials to serve as the manager for an activity. See AR 380-5 for basic responsibilities. Also refer to AR 380-381(C) for security managers of special access programs.

Sensitive activities

Sensitive activities are special access or codeword programs, critical research and development efforts, operational or intelligence activities, cover, special plans, special activities, sensitive support to non-Army agencies and/or activities excluded from normal staff review and oversight.

Sensitive information

Sensitive information is information requiring special protection from disclosure that could cause compromise or threat to our national security, an Army organization, activity, family member, DA civilian, or DOD contractor. Sensitive information refers to unclassified information while sensitive compartmented information (SCI) refers to classified information. Examples which may be deemed sensitive include but are not limited to: personal information; structuring; manning; equipment; readiness; training; funding; sustaining; deploying; stationing; morale; vulnerabilities; capabilities; administration and personnel; planning; communications; intelligence, counterintelligence, and security; logistics; medical; casualties and acquisition plans.

Sensitive Compartmented Information (SCI)

Information or material requiring special controls for restricted handling within compartmented intelligence systems and for which compartmentalization is essential. SCI rules are established by the Director of Central Intelligence and are covered in DOD C-5105.21-M-1.

Sources of data

Materials, conversations and actions that provide information and indicators. The sources are as follows:

- a. Protected sources. Friendly personnel, documents, material and so forth, possessing classified or

sensitive data which are protected by personnel, information, physical, crypto, emission and computer security measures.

- b. Open sources. Oral, documentary, pictorial and physical materials accessible to the public.
- c. Detectable actions. Physical actions or entities and emissions or other phenomena that can be

observed, imaged or detected by human senses or by active and passive sensors.

Special Access Program (SAP)

A sensitive activity, approved in writing by the Secretary of Defense. It imposes extraordinary security measures to control access and provide protection of extremely sensitive information in addition to the provisions of AR 380-5. The controls depend on the criticality of the program and the intelligence threat.

TEMPEST

An unclassified name referring to investigations and studies of compromising emanations. Sometimes used synonymously for the term "compromising emanations."

Threat

Capability of a potential adversary to limit or negate mission accomplishment or to neutralize or reduce the effectiveness of a current or projected organization or material item. Two types of threat information are required:

- a. Intelligence collection threat (efforts by adversary to gain information).
- b. Combat capability threat (adversary forces' weapons systems which the U.S. Army will face on the

battlefield).

User agency (UA)

A User Agency is a government customer of private industry. Any Army command, activity, or installation that enters into a contract with private industry is a User Agency. Since UA may not develop its own contracting requirements, the term Requiring Activity refers to an organization that has a specific requirement for goods and/or services and requests the initiation of, and provides funding for an assisted or direct acquisition to fulfill that requirement.