

Headquarters  
Eighth Army  
Unit #15236  
APO AP 96205-5236

Army in Korea  
Regulation 530-1

1 July 2016

Operations and Signal Security  
OPERATIONS SECURITY (OPSEC)

---

**\*This regulation supersedes Army in Korea Regulation 530-1, dated 9 January 2010.**

---

FOR THE COMMANDER:

WILLIAM D. TAYLOR  
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 wartime planning, training and miscellaneous activities to be used by Eighth Army (8A) units, off-peninsula units training in Korea and activities supported by 8A.

**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) 8A, off shore Army units training in Korea and units located in Korea supported by inter-service support agreements with HQ 8A.

**Supplementation.** Supplementation of this regulation and issuance of command and local forms is prohibited unless prior approval is obtained from HQ 8A, G33, OPSEC Officer, Unit #15236, APO AP 96205-5236.

**Forms.** AK forms are available at [http://8tharmy.korea.army.mil/g1\\_ag/](http://8tharmy.korea.army.mil/g1_ag/).

**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>.

**Army internal control process.** This regulation contains internal control provisions in accordance with AR 11-2 and identifies key internal controls that must be evaluated (see appendix O).

**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 8A, G33, OPSEC Officer, APO AP 96204.

**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, 8A G33 Current Operations, PSC 303 Box 27, APO AP 96204-5236.

**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. Responsibilities
- 1-5. Definitions
- 1-6. Requirement
- 1-7. Application
- 1-8. Proponent

### **Chapter 2**

#### **Responsibilities, page 4**

- 2-1. 8A Commander
- 2-2. All Commanders
- 2-3. 8A Staff Directorates and Chiefs of Special Staffs
- 2-4. 8A G1 (Personnel)
- 2-5. 8A G2 (Intelligence)
- 2-6. 8A G3/5/7 (Operations and Maneuver)
- 2-7. 8A G4 (Sustainment)
- 2-8. 8A G6 (Command and Control)
- 2-9. 8A G9 (Civil Affairs Operations)
- 2-10. 8A IG (The Inspector General)
- 2-11. 8A PAO (Public Affairs Office)
- 2-12. Primary and Special Staff not previously mentioned
- 2-13. All 8A Personnel (active and reserve component, DA civilians, and Civilian Contractors)
- 2-14. OPSEC Program Managers, Officers, and Coordinators

### **Chapter 3**

#### **Policy and Procedures, page 9**

- 3-1. General
- 3-2. OPSEC Programs
- 3-3. Program Awareness And Training Product Promotion
- 3-4. Threat Analysis Support to OPSEC

### **Chapter 4**

#### **Training Requirements, page 12**

- 4-1. Overview
- 4-2. Training Programs
- 4-3. OPSEC and External Official Presence Training
- 4-4. Joint and Interagency Training

### **Chapter 5**

#### **OPSEC Review, Assessment, and Survey, page 14**

##### Section I. OPSEC Review

## **CONTENTS (CONT)**

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

### Section II. OPSEC Assessment

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

### Section III. OPSEC Survey

- 5-5. General
- 5-6. Procedures
- 5-7. Planning Phase
- 5-8. Field Survey Phase
- 5-9. Analysis and Reporting Phase

## **Chapter 6**

### **OPSEC Contractual Documents Review Requirements, *page 22***

- 6-1. Overview
- 6-2. Policies and Procedures

## **Chapter 7**

### **Special Access Programs, *page 23***

- 7-1. Overview
- 7-2. Policy

## **Appendixes, *page 25***

- A. References
- B. The Operations Security Process
- C. Sample Critical Information
- D. Operations Security Indicators
- E. The Threat
- F. Sample Operations Security Measures
- G. Operations and Security Relationships to Security Programs
- H. Standard Duty Description for OPSEC Program Managers, Officers, and Coordinators
- I. Annual Operations Security Report Format
- J. Annual Army Operations Security Achievement Awards Program
- K. 8A Staff and Major Subordinate Commands
- L. Information That May Be Exempt from Release under the Freedom of Information Act
- M. Format for Operations Security Annex/Appendix/Tab to Operation Plan/Operation Order
- N. Format for Operations Security Documents
- O. Internal Control Evaluation
- P. OPSEC Assessment
- Q. OPSEC Compromise Procedures
- R. FOIA Cover Sheet
- S. Social Media Checklist

## **CONTENTS (CONT)**

### **Figure Lists**

- Figure 5-1. OPSEC Survey Planning Phases, *page 17*
- Figure 5-2. Generic Functional Outline/Profile, *page 19*
- Figure 5-3. Example OPSEC Survey Report Format, *page 22*
- Figure I-1. 8A MSC Annual OPSEC Report Format, *page 57*
- Figure I-2. 8A Annual OPSEC Report Format, *page 63*

**Glossary, *page 79***

## **Chapter 1**

### **Introduction**

#### **1-1. Purpose**

To establish policy and procedures for Operations Security (OPSEC) within Eighth Army (8A), its major subordinate commands (MSC), 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. Responsibilities**

Responsibilities are listed in chapter 2 and appendix H. Responsibilities referring to commanders and similar terms are equally applicable to equivalent management and supervision positions in organizations that do not employ a traditional military command structure.

#### **1-5. Definitions**

a. Operations Security: As defined in Army Regulation 530-1 (Operations Security), OPSEC is a process of identifying critical information and analyzing friendly actions attendant to military operations and other activities to—

- (1) Identify those actions that can be observed by adversary intelligence systems.
- (2) Determine indicators and vulnerabilities that adversary intelligence systems might obtain to be able to interpret or piece together to derive critical information in time to use against U.S. and/or friendly missions and poses an unacceptable risk.
- (3) Select and execute measures that eliminate the risk to friendly actions and operations or reduce to an acceptable level.

b. OPSEC protects sensitive and/or critical information from adversary observation and collection in ways that traditional security programs cannot. While these programs, such as Information Assurance (IA), protect classified information, they cannot prevent all indicators of critical information, especially unclassified indicators, from being revealed.

c. In concise terms, the OPSEC process identifies the critical information of military plans, operations, and supporting activities and the indicators that can reveal it, and then develops measures to eliminate, reduce, or conceal those indicators. It also determines when that information may cease to be critical in the lifespan of an organization's specific operation.

(1) Critical information, formerly known as essential elements of friendly 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.

(2) Critical information consists of specific facts about friendly capabilities, activities, limitations (includes vulnerabilities), and intentions (CALI) needed by adversaries for them to plan and act effectively so as to degrade friendly mission accomplishment.

(3) Critical information is information that is vital to a mission that if an adversary obtains it, correctly analyzes it, and acts upon it; the compromise of this information could prevent or seriously degrade mission success.

(4) Critical information can either be classified or unclassified depending upon the organization, activity, or mission. Critical information that is classified requires OPSEC measures for additional protection because it can be revealed by unclassified indicators. Critical information that is unclassified especially requires OPSEC measures because it is not protected by the requirements pertaining to classified 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.

(5) An OPSEC compromise is the disclosure of sensitive and/or critical information that jeopardizes a unit's ability to execute its mission or to adequately protect its personnel and/or equipment or effects national security.

(6) For sensitive and/or critical information that has been compromised and is available in open sources, the public domain should not be highlighted or referenced publicly outside of intra-governmental or authorized official communications, because these actions provide further unnecessary exposure of the compromised information. Personnel should not respond to queries to deny or confirm the validity of sensitive information that has been compromised or released to the public. Notify your organization's OPSEC officer and security manager of all OPSEC compromises.

#### **1-6. Requirement**

a. The National OPSEC Program outlined in National Security Decision Directive (NSDD) 298 requires each executive department and agency with a national security mission to have an OPSEC program. Likewise, Department of Defense Directive (DoDD) 5205.02E supports the national program and requires each Department of Defense (DoD) component to have an OPSEC program.

b. OPSEC 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 and full implementation of two approaches to protection—

(1) OPSEC to deny adversaries critical information and indicators of sensitive information.

(2) Traditional security programs to deny adversaries classified, sensitive, and/or critical information include—

- (a) Information security.
- (b) Information assurance.
- (c) Electronic security.
- (d) Emission security.
- (e) Military deception.
- (f) Physical security.

- (g) Program protection planning.
- (h) Personnel security.
- (i) Industrial security.

c. OPSEC provides a 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.

## **1-7. Application**

a. Operations security awareness and execution is crucial to Army success. OPSEC is applicable to all personnel and all 8A 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 conducting operations, exercises, tests, or activities.

(1) The 8A 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 (JP) 3-13.3. In Joint and Army operations, OPSEC is a core information-related capability as prescribed in JP 3-13.3 and FM 3-13, and a component of Protection.

(2) Information Operations integrate OPSEC, military deception, psychological operations (PSYOP), electronic warfare (EW), and computer network defense. The Information Operation (IO) supporting capabilities include information assurance (IA) and counterintelligence (CI) 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 8A 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.

## **1-8. Proponent**

The Assistant Chief of Staff (ACoS) G3/5/7 is the 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. Eighth Army Commander**

The 8A Commander will develop and implement a functioning, active, and documented (formal) OPSEC program. To develop and implement a formal OPSEC program, the 8A Commander will—

a. Appoint a Command OPSEC program manager in writing.

(1) The 8A 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 Department of Army (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. Republic of Korea (ROK) government, military, civilian, and contractor personnel and Korean Augmentees to the United States Army (KATUSA) will not be assigned as the command's OPSEC program manager or OPSEC officer.

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 8A OPSEC program manager maintains routine contact with the Army, United States Army Pacific (USARPAC), and USFK OPSEC program managers. The 8A OPSEC program manager will provide updates, status reports, OPSEC issues, OPSEC compromises, lessons

learned, and initiatives, requests for support, recommendations, personnel turnover, and verification of contact information, media contacts, and so forth.

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

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

f. Ensure that their tenant units coordinate with the garrison OPSEC Officer and participate in the garrison installation-level OPSEC working groups as required.

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, USARPAC, USFK, GCC, and 8A OPSEC (or Protection) working groups and 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 standing operating procedure (SOP). At a minimum, the OPSEC 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 and staff sections determine their critical information, develop OPSEC measures to protect their critical information, and provide this information to a higher echelon OPSEC program.

(6) Regardless of the level of implementation of OPSEC programs, every staff organization must have its own OPSEC program or be covered under a higher echelon staff organization's OPSEC program.

(7) Ensure their OPSEC program or OPSEC measures are coordinated and synchronized with supported organizations and supporting higher command's OPSEC program and security programs, such as information security (INFOSEC), IA, physical security, and force protection.

(8) Ensure all official information released to the public domain receives an OPSEC review by a level II trained OPSEC PM, OPSEC officer, or OPSEC coordinator prior to dissemination.

(9) Ensure all OPSEC program documents are reviewed at least annually to ensure changes in mission, threat, critical information lists (CILs), or OPSEC measures are reflected in plans and SOPs in a timely manner.

(10) Ensure 8A and subordinate units participate in garrison installation-level OPSEC working groups, as required, in accordance with AR 530-1, paragraph 2-19.

(11) Submit annual OPSEC report (.pdf file) to the 8A program manager in accordance with appendix I, AR 530-1, no later than 1 November.

### **2-3. 8A Staff Directorates and Chiefs of Special Staffs**

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

### **2-4. 8A G1 (Personnel)**

a. The Personnel Directorate 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.

c. Utilize the 8A Critical Information List (CIL), the five-step OPSEC process, and the 8A FOIA request OPSEC checklist to screen all Freedom of Information Act (FOIA) requests.

d. Provide completed copies of the 8A FOIA request OPSEC Cover Sheet to the 8A OPSEC program manager (see appendix R, FOIA Cover Sheet, to this regulation).

e. Appoint an OPSEC officer in writing in accordance with appendix H-6, paragraph b4 of this regulation and ensure Level II certification within 90 days of appointment.

### **2-5. 8A G2 (Intelligence)**

a. Assist other 8A 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. Maintain and update annually, a written regional threat assessment that integrates OPSEC and adversary information collection capabilities. The threat assessment will be made available to the 8A OPSEC program manager for inspections. The threat assessment should be coordinated

with 8A Major Subordinate Commands (MSCs) to ensure subordinate unit threat assessments are synchronized across the force to the extent practical.

c. Provide overall threat assessment to forces in addition to threat assessment to specific operations.

d. Serve as the 8A staff proponent for signal intelligence (SIGINT), human intelligence (HUMINT), imagery intelligence (IMINT), measurement & signal intelligence (MASINT), and open source intelligence (OSINT) supporting OPSEC.

e. Recommend OPSEC measures to 8A senior leaders and the 8A OPSEC program manager.

f. Appoint an OPSEC officer in writing in accordance with appendix H-6, paragraph b4 of this regulation and ensure Level II certification within 90 days of appointment.

## **2-6. 8A G3/5/7 (Operations and Maneuver)**

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 Headquarters, Department of the Army (HQDA), 1st Information Operations (IO) Command, Operations Security Element (OSE) and Inter-Agency OPSEC Support Staff (IOSS) and submit request through USARPAC or HQ USFK CJ39 (dependent on command relationship at the time).

c. Ensure appropriate OPSEC measures are taken within 8A to preserve essential secrecy.

d. Publish protective measures to be implemented in Operation Plans and Operation Orders.

e. Ensure OPSEC training is conducted in accordance with regulations and doctrine.

f. Serve as chairperson during OPSEC Working Groups, when conducted.

g. Attend quarterly or monthly 8A G34 Protection working groups.

h. Recommend 8A OPSEC training objectives to the Commanding General for major training events and exercises.

i. Appoint an OPSEC officer in writing in accordance with appendix H-6, paragraph b4 of this regulation and ensure Level II certification within 90 days of appointment.

## **2-7. 8A G4 (Sustainment)**

a. Analyze logistics reports and procedures to identify indicators compromising 8A 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.

c. Recommend 8A OPSEC training objectives to the Commanding General for major training events and exercises.

d. Appoint an OPSEC officer in writing in accordance with appendix H-6, paragraph b4 of this regulation and ensure level II certification within 90 days of appointment.

**2-8. 8A G6 (Command and Control)**

a. Assist the G2 (Intelligence) and G3/5/7 (Operations and Maneuver) in developing the Mission Command (MC) appendix for 8A OPLANS, CONPLANS and exercise directives.

b. Establish emission control and wartime reserve modes for 8A communication emitters.

c. Enforce procedures for password and login protection.

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

e. Recommend 8A OPSEC training objectives to the Commanding General for major training events and exercises.

f. Appoint an OPSEC officer in writing in accordance with appendix H-6, paragraph b4 of this regulation and ensure level II certification within 90 days of appointment.

**2-9. 8A G9 (Civil Affairs Operations)**

a. Assist the G2 (Intelligence) in recognizing possible human intelligence (HUMINT) activities supporting OPSEC (i.e. any information pertaining to OPSEC issues).

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

c. Appoint an OPSEC officer in writing in accordance with appendix H-6, paragraph b4 of this regulation and ensure Level II certification within 90 days of appointment.

**2-10. 8A IG (The Inspector General)**

a. The Inspector General will ensure that OPSEC is an item of interest in inspections of organizations throughout 8A, particularly during major exercises and training events.

b. Appoint an OPSEC officer in writing in accordance with appendix H-6, paragraph b4 of this regulation and ensure Level II certification within 90 days of appointment.

**2-11. 8A PAO (Public Affairs Office)**

a. Ensure that OPSEC has been considered in the preparation of all public releases of information. The 8A CIL and five-step OPSEC process will be used when preparing information for public release.

b. Ensure an OPSEC Level II trained official reviews all publicly released information.

c. Conduct prior coordination with the OPSEC officer and PSYOP representative before releasing operational or mission related information to prevent disclosure of critical information.

d. Assist the G2 (Intelligence) in recognizing possible open source intelligence (OSINT) activities supporting OPSEC (i.e. any information pertaining to OPSEC issues).

#### **2-12. Primary and Special Staff not previously mentioned**

Appoint an OPSEC officer in writing in accordance with appendix H-6, paragraph b4 of this regulation and ensure level II certification within 90 days of appointment.

#### **2-13. All 8A Personnel (active component, reserve component, DA civilians) and Civilian Contractors**

a. Know what their organization considers to be sensitive and/or critical information, where it is located, who is responsible for it, how to protect it, why it needs to be protected, and who the unit OPSEC officer is.

b. Do not publicly disseminate or publish photographs displaying sensitive and/or critical information.

c. Do not publicly reference, disseminate, confirm, publish, or further propagate sensitive and/or critical information that has already been compromised, as this provides further unnecessary exposure of the compromised information and may serve to validate it. See AR 380-5 for further guidance.

d. Implement OPSEC measures as determined by the commander or OPSEC officer to protect sensitive and critical information from unauthorized disclosure.

e. Actively encourage others (including family members and Family Readiness Groups (FRGs)) to protect sensitive and/or critical information.

f. Handle any attempt by unauthorized personnel to solicit sensitive or critical information as a Threat Awareness and Reporting Program (TARP) 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.

g. Become familiar with AR 340-21 to prevent disclosure of personal or private information.

h. Destroy (burn, shred, and so forth) sensitive and/or critical information that is no longer needed to prevent the inadvertent disclosure and reconstruction of this material per applicable standards. See AR 380-5 for further guidance.

#### **2-14. OPSEC Program Managers, Officers, and Coordinators**

Perform duties and responsibilities outlined in appendix H to this regulation.

### **Chapter 3 Policy and Procedures**

#### **3-1. General**

Operations Security applies throughout the range of military operations across the spectrum of conflict to all 8A operations. All 8A 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 document(s) (policy, plan, or 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 by the commander or designated approval authority.

(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) 8A: 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 in writing (in the appointment memorandum or order) 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. The threat analysis may be of a higher classification than the SOP and must be safeguarded accordingly.

(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. Programs must be reviewed annually.

e. 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. Program Awareness and Training Product Promotion**

a. Active promotion of the OPSEC program is the responsibility of commands. Units, staff elements, and installations are encouraged to develop their own OPSEC training products and use all suitable techniques of publicity and promotion consistent with law and within funds available.

b. As part of promotional efforts, commanders/directors at all levels should—

(1) Advertise the OPSEC program through posters, billboards, inserts in bulletins, or other media which frequently reach Soldiers, DA civilians, contractors, and Family members.

(2) Develop slogans, logos, and other materials designed to call attention to the OPSEC program.

(3) Note that appropriated funds generally may not be used to purchase promotional items to be given away to government employees, members of the public, or others. Such expenditures can only be justified under very unusual and unique circumstances, and must always be reviewed by servicing legal counsel before any funds are obligated for such a purpose.

### **3-4. Threat Analysis Support to OPSEC**

8A G-2 (Intelligence) will provide threat analysis support to OPSEC through MSC intelligence channels. When this is not practical or possible, units will forward their requirements through proper channels to the appropriate threat analysis center. Threat assessments will be reviewed annually, at a minimum, for currency.

## **Chapter 4 Training Requirements**

### **4-1. Overview**

For OPSEC to be effective, all 8A personnel (Soldier, DA Civilian, and DOD contractors) must be aware of OPSEC and understand how OPSEC complements traditional security programs. All 8A personnel must know how to apply and practice OPSEC in the performance of their daily tasks. OPSEC must become a mindset of all 8A 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 in-processing and 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 8A 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 8A 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:

(2) 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.

(a) Understanding what is critical information.

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

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

(d) 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 HQDA OPSEC Officers Course, conducted by the OPSEC Support Element (OSE), or the IOSS equivalent to be Level II certified. Personnel authorized or required to conduct OPSEC reviews from contract solicitation documents, and so forth, must also complete the OPSEC Level II certification. OPSEC coordinators, Web masters, PAOs, FOIA, speech writers, FRsAs, or any other personnel who interact with the public on a regular basis will receive external official presence (EOP) training or attend a Level II OPSEC officer's course, so long as they are appointed in writing by the Commander (or designated authority) and possess a valid U.S. secret clearance (KATUSAs and ROK civilian employees serving in U.S. units may be eligible for training if they possess a ROKA equivalent security clearance and the 8A OPSEC Program Manager has obtained permission from 1<sup>st</sup> Information Operations Command).

c. *OPSEC Level III Certification Training.* The Army OSE offers Army Level III OPSEC instructor certification. OPSEC PMs at ACOMs, ASCCs, DRUs, corps, and installations may opt to receive OPSEC Level III training. Refer to section 4-2, Training Programs, AR 530-1 for further information.

#### **4-3. OPSEC and External Official Presence Training**

While the Internet is a powerful tool to convey information quickly and efficiently, it can also provide adversaries a potent instrument to obtain, correlate, and evaluate an unprecedented volume of aggregate information regarding U.S. capabilities, activities, limitations, and intentions (CALI).

a. All commanders will ensure those personnel who publish or input information on External Official Presence (EOP) sites receive *OPSEC for EOP Operators* training. This will be PAO/OPSEC training specific to persons whose duties include operating or maintaining EOP sites. All Soldiers, DA civilians, and contractors who post or maintain information or documents on the public domain for official purposes are required to take this computer-based training. The *OPSEC for EOP*

Operators training course may be found on the US Army Information Assurance Virtual Training website at: <https://iatraining.us.army.mil/html/student.htm#reqtype=courselist>.

b. Per AR 25–1, OPSEC officers and PAOs are required to conduct quarterly reviews of publicly accessible and registered military and/or government Web sites to ensure the information available does not compromise OPSEC. OPSEC PMs/officers will conduct an OPSEC review, and the PAO will prepare information for release in all forms of media (for example, print, Web posting, and public speeches).

#### **4–4. Joint and Interagency Training**

a. *Interagency OPSEC support staff.* The IOSS supports the National OPSEC Program by providing tailored training, assisting in program development, producing multimedia products, and presenting conferences for the defense, security, intelligence, research and development, acquisition, and public safety communities. Its mission is to help government organizations develop their own, self-sufficient OPSEC programs in order to protect U.S. programs and activities. IOSS is recognized as the standard for government OPSEC programs and provides subject matter expertise to the Department of Defense.

(1) IOSS offers a multitude of OPSEC training aids which are available to all OPSEC officers (see <https://www.iad.gov/ioss/index.cfm>).

(2) 8A personnel may receive training from the IOSS. However, the training courses offered by the IOSS provide a broader perspective of OPSEC for the Joint and interagency level while Army OPSEC training is oriented specifically to an Army audience.

## **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. Unit and staff element standing operating procedures will state which documents automatically go to the OPSEC officer for a review. News releases, Web content, and responses to FOIA and Privacy Act requests are examples of products that require automatic review by a public affairs-qualified NCO/DA civilian/officer or OPSEC officer.

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 70-1, AR 70-31, and MIL STD 1806 for contractors producing technical information for the U.S. government.

d. All official, publicly accessible, organizational Web sites must have an OPSEC Web site review to ensure no operationally sensitive and/or critical information is posted to or contained thereon, as per AR 25-1 and AR 25-2. The OPSEC Web site review is the responsibility of the Webmaster/maintainer, in coordination with the OPSEC officer, PAO, and other appropriate designees (to include, but not limited to, security, intelligence, and legal personnel). The unit CIL approved by the commander, will be used as the basis for determining releasability.

## **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. Each 8A MSC and staff directorate OPSEC PM/officer will conduct an annual self-assessment to determine the effectiveness of his or her OPSEC program, and as a minimum, assess the status of the following:

- (1) Unit personnel's knowledge of critical information or publication of the CIL.
- (2) Unit personnel's knowledge of the collection threat to the unit.
- (3) OPSEC measures in place to protect identified critical information.
- (4) The status of OPSEC training.

b. At each command level, the organization must conduct an OPSEC assessment of subordinate. The command OPSEC officer submits a written assessment with results and recommendations to the assessed unit commander or commander that directed the assessment. As a minimum, the following will be assessed:

- (1) Identification of critical information.
- (2) Unit personnel's knowledge of critical information or publication of the CIL.
- (3) Unit personnel's knowledge of the collection threat to the unit.
- (4) OPSEC measures in place to protect identified critical information.
- (5) The status of OPSEC training.
- (6) Application of a formal OPSEC checklist based on restrictions in existing laws, statutes, regulation and policy, including any specific requirements applicable only to the assessed organization and/or other organizations of its type.

(a) Each headquarters will develop and publish an OPSEC checklist (or checklists, if differing OPSEC requirements apply to different subordinate organizations) as part of the organizational inspection program (OIP)/command inspection program (CIP).

(b) This does not preclude OPSEC assessments from being conducted other than as part of the annual CIP.

c. Use appendix P OPSEC Assessment as a guide to conduct an OPSEC assessment.

### **Section III. OPSEC Survey**

#### **5-5. General**

a. A survey is the application of the OPSEC methodology by a team of experts to conduct a detailed analysis of activities associated with a specific organization, operation, activity, exercise, or support function by employing the known collection capabilities of potential adversaries. This evaluation should focus on the agency's ability to adequately protect critical information from adversary intelligence exploitation during planning, preparation, execution, and post-execution phases of any operation or program. Surveys must be conducted every three years or as requested by the commander or higher headquarters.

b. OPSEC surveys are personnel, resource, and time-intensive and should only be conducted as triennially required (per the preceding paragraph) or when deemed necessary by the commander. Extremely sensitive programs, activities, or operations where the slightest compromise will result in mission failure and/or extreme damage to national security are rare examples of where additional OPSEC surveys (i.e., in addition to the required triennial survey) are more likely to be warranted.

c. Activities that warrant additional OPSEC surveys include, but are not limited to, RDT&E, acquisitions, treaty verification, nonproliferation protocols, international agreements, force protection operations, special assess programs, and activities that prepare, sustain, or employ U.S. Military Forces over the range of military operations.

d. The commander will determine whether a command survey or formal survey will be performed.

#### **5-6. Procedures**

a. The objective is to identify OPSEC vulnerabilities in operations or activities that an adversary could exploit to degrade friendly effectiveness or the element of surprise. The survey helps the commander to evaluate OPSEC measures and take further action to protect critical information.

b. 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.

c. The 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, or in compromising ongoing research and development programs and activities.

d. A survey will not serve as an inspection of the effectiveness of a command's security programs or adherence to security directives. Each survey is unique, as it reflects the operation or activity it analyzes. Nevertheless, there are common procedures, which subsequent paragraphs discuss.

(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. Additionally, if the survey is conducted by the Army OSE, a report is provided to the requesting commander.

e. There are two types of surveys—

(1) A command survey concentrates on events that 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 organizational lines with prior coordination). The survey team includes members from both inside and outside the surveyed organization. A letter or message initiates the formal survey. It states the subject, team members, and dates of the survey. It can also list organizations, activities, and locations. Contact the Army OSE for more information.

---

<p><b>1. Planning Phase</b></p> <ul style="list-style-type: none"><li>a. Determine the scope of the survey.</li><li>b. Select team members.</li><li>c. Become familiar with survey procedures.</li><li>d. Determine the foreign intelligence threat.</li><li>e. Understand the ops or activity to be surveyed.</li><li>f. Conduct empirical studies.</li><li>g. Develop a functional outline.</li><li>h. Determine preliminary friendly vulnerabilities.</li><li>i. Announce the survey.</li></ul>	<p><b>2. Field Survey Phase.</b></p> <ul style="list-style-type: none"><li>a. Make an entrance brief.</li><li>b. Receive a command brief.</li><li>c. Collect data and refine functional outline.</li><li>d. Make an exit brief.</li></ul> <p><b>3. Analysis and Reporting Phase.</b></p> <ul style="list-style-type: none"><li>a. Correlate data.</li><li>b. Identify vulnerabilities.</li><li>c. Prepare final report.</li></ul>
--	---

**Figure 5-1. Survey Planning Phases**

---

### **5-7. 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 CIL. 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 CIL, 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:**

---

i. 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.

#### **5-8. 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.

### **5-9. 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.

---

<p><b>I. OVERVIEW</b></p> <p>A. <i>Background. Origin, purpose, scope of survey; threat/vulnerability assessment.</i></p> <p>B. <i>Conduct of Survey. Brief discussion of methodology; team composition; major units or activities visited; time-frame of survey.</i></p> <p><b>II. SUMMARY OF SIGNIFICANT FINDINGS</b></p> <p><i>Extract of major findings from paragraph III below.</i></p> <p><b>III. ANALYSIS, CONCLUSIONS. AND FINDINGS</b></p> <p>A. <i>The body of the report. Discussions and findings may be listed chronologically, by command, or chronologically within commands.</i></p> <p>B. <i>Suggested format for each finding:</i></p> <ol style="list-style-type: none"><li><i>Finding.</i></li><li><i>Analysis and Discussion.</i></li><li><i>Conclusion or Recommendation.</i></li></ol>
--

**Figure 5-3. Example OPSEC Survey Report Format**

---

## **Chapter 6**

### **OPSEC Contractual Documents Review Requirements**

#### **6-1. Overview**

All 8A acquisition programs and government contracts will employ OPSEC to protect classified, critical, and sensitive information. 8A unit, organization, and staff element OPSEC officers will review all contractual documents to determine what OPSEC measures are required to protect critical and/or sensitive information. OPSEC measures will be integrated into contract documents and coordinated with the government contracting activity to include OPSEC measures in the solicitation package and resultant contract using the antiterrorism (AT)/OPSEC coversheet.

#### **6-2. Policies and Procedures**

a. Commanders will establish procedures to document the review of all contractual documents by using the AT/OPSEC Desk Reference coversheet to indicate review by the unit, organization, or staff element OPSEC officer. If the unit, organization, or staff element does not have an appointed OPSEC officer, the unit, organization, or staff element's higher headquarters OPSEC officer will provide the OPSEC review.

b. For unclassified contracts, the unit, organization, or staff element OPSEC officer will review contractual documents to determine if any specific OPSEC measures are required in a contract. The unit, organization, or staff element OPSEC officer will integrate any needed OPSEC measures into the Performance Work Statement (PWS), the statement of work (SOW), or the statement of

objectives (SOO) in sufficient detail to ensure complete contractor understanding of the exact OPSEC measures required by 8A regulation. The government contracting activity will integrate the OPSEC measures into the solicitation package and resultant contract. If the contract is modified or given another option year, this review process will be repeated to ensure required OPSEC measures remain current and relevant throughout the lifecycle of the contract.

c. The unit, organization, or staff element OPSEC officer will also perform an OPSEC review to identify any critical and/or sensitive information associated with the contract and, if found, determine specific OPSEC measures required in the contract prior to submitting the contractual documents to the government contracting activity. The unit, organization, or staff element's published CIL and OPSEC measures will provide the basis for this review. The unit, organization, or staff element's OPSEC officer will coordinate for document modifications to eliminate or minimize any discovered critical and/or sensitive information. If critical information is part of the contractual document(s) or the unit, organization, or staff element's OPSEC officer believes any identified sensitive information should not be removed because it maintains the integrity of the contract, the unit, organization, or staff element's OPSEC officer will ask the government contracting activity to release the contractual document(s) in an online secure environment with controlled access and to ensure the solicitation package does not contain any critical and/or sensitive information, but instead refers to the secure location where the full document(s) can be accessed by appropriate personnel.

d. For classified contracts, the unit OPSEC officers will coordinate with the unit's G-2/S-2 Intelligence section, or through their chain of command for an industrial security specialist, or submit a request to an appropriate outside agency for industrial security support for completion of a DD Form 254 (Department of Defense Contract Security Classification Specification). The industrial security specialist completes the DD Form 254 which is used to convey security requirements in a classified contract. The industrial security specialist will review the SOW, SOO, or PWS to ensure the appropriate security clauses and/or language are contained therein to address the protection of classified information. The industrial security specialist ensures the OPSEC measures contained in the SOW, SOO, or PWS are also reflected on the DD Form 254. The industrial security specialist will forward the fully executed DD Form 254 to the requiring activity (RA) for submission to the government contracting activity. If the contract is modified or given another option year, this process will be repeated to ensure the DD Form 254 remains current and relevant throughout the lifecycle of the contract.

## **Chapter 7**

### **Special Access Programs**

#### **7-1. Overview**

A Special Access Program (SAP) is a security program established under EO 13526 and authorized by the Secretary of Defense to administer extraordinary security measures to control access and provide protection of extremely sensitive information in addition to the provisions of AR 380-5 for classified information. The SAP manager, director, or commander is responsible for OPSEC for the SAP.

#### **7-2. Policy**

Each SAP will have a functioning OPSEC program with an appointed OPSEC officer from conception to disestablishment.

- a. The SAP OPSEC officer will manage and document the SAP's OPSEC program.
- b. Each SAP will have a written OPSEC plan or annex.

c. The 8A G34 (Protection), in coordination with the 8A G-2 and 8A G33, will provide policy guidance and oversight for SAP OPSEC procedures.

d. The 8A G34 (Protection) will include the 8A OPSEC PM in any SAP or Defense Critical Infrastructure Program (DCIP) special working groups.

## **Appendix A References**

### **Section I. Required Publications**

AK Pam 1-201, Army Inspection Policy (Cited in para 2-1e)

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

AR 25-1, Army Information Technology (Cited in appendix G-3, para a)

AR 25-2, Information Assurance (Cited in appendix G-3, para a)

AR 25-30, The Army Publishing Program

AR 25-55, The Department of the Army Freedom of Information Act Program (Cited in appendix L-2)

AR 70-1, Army Acquisition Policy

AR 70-31, Standards for Technical Reporting

AR 340-21, The Army Privacy Program

AR 350-1, Army Training and Leader Development

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

AR 380-27, Control of Compromising Emanations

AR 380-40, Safeguarding and Controlling Communications Security Material (U)

AR 380-49, Industrial Security Program

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

AR 381-12, Threat Awareness and Reporting Program (Cited in para 2-12b)

AR 530-1, Operations Security (OPSEC)

DODD 5205.02E, DOD Operations Security Program (Cited in paras 1-6a)

DOD 5205.02-M, DOD Operations Security (OPSEC) Program Manual

DoDI 5200.39, Critical Program Information (CPI) Identification and Protection within Research, Development, Test, and Evaluation (RDT&E)

DoD 5200.01, DoD Information Security Program

FM 3-13, Inform and Influence Activities

Joint Publication 3-13.3, Operations Security

## **Section II. Related Publications**

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

AR 360-1, The Army Public Affairs Program

AR 380-49, Industrial Security Program

AR 380-53, Communications Security Monitoring

AR 380-67, Personnel Security Program

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

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

AR 381-20, The Army Counterintelligence Program

AR 381-102 (S), U.S. Army Cover Program (U)

AR 525-21 (S), Military Deception (U)

AR 715-30, Secure Environment Contracting

CJCSI 3213.01D, Joint Operations Security

DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure

DoDD 5000.01, The Defense Acquisition System

DoDD 5230.25, Withholding of Unclassified Technical Data from Public Disclosure

DoDD 5400.07, DOD Freedom of Information Act Program

DoDI 5000.02, Operation of the Defense Acquisition System

DoDI 5205.11, Management, Administration, and Oversight of DoD Special Access Programs (SAPs)

DoDI 5230.24, Distribution Statements on Technical Documents

DoD 3020.45-V3, Defense Critical Infrastructure Program (DCIP) Security Classification Manual (SCM)

DoDM 5205.02-M, DoD Operations Security (OPSEC) Program Manual

DODD 5205.07, Special Access Programs (SAP) Policy

DOD 5220.22-M, National Industrial Security Program Operating Manual

Executive Order 13222, Continuation of Export Control Regulation

EO 13526, Classified National Security Information

Joint Publication 2-0, Joint Intelligence

National Security Decision Directive 298, National Operations Security Program

**Section III  
Prescribed Forms**

Contract Requirements Package Anti-terrorism/Operations Security Review Cover Sheet

**Section IV  
Referenced Forms**

DA Form 11-2, Internal Control Evaluation Certification

DD Form 254, Department of Defense Contract Security Classification Specification

## **Appendix B**

### **The Operations Security Process**

#### **B-1. Overview**

The OPSEC process consists of five steps which can apply to any plan, operation, program, project, or activity. These steps provide a framework for the systematic process necessary to identify, analyze, and protect sensitive information. The process is continuous and assessments should occur frequently throughout an operation. 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.
- b. Analysis of threats.
- c. Analysis of vulnerabilities.
- d. Assessment of risk.
- e. Application of OPSEC measures.

#### **B-2. Identification of Critical Information**

The purpose of this step is to determine what needs protection. This is one of the most difficult steps of the five-step process and is the most important to accomplish. OPSEC cannot protect everything, so the most important items should be afforded the greatest efforts of protection. The OPSEC officer, in conjunction with other staff officers' input, develops the unit or organization's critical information and provides it to the commander, director, or an individual in an equivalent position for approval.

a. Critical information consists of specific facts about friendly intentions, capabilities, limitations, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.

(1) Critical information is information that is vital to a mission that if an adversary obtains it, correctly analyzes it, and acts upon it; the compromise of this information could prevent or seriously degrade mission success.

(2) Critical information can be classified information or unclassified information. OPSEC measures protect the unclassified indicators that can reveal classified information.

(3) Critical information that is unclassified requires OPSEC measures, because it is not protected by the stringent, well defined requirements provided to classified information.

(4) 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.

b. There are several sources which can help the OPSEC officer determine the unit or organization's critical information.

(1) The supporting intelligence element will provide information on the adversary and its intelligence requirements. Known tasking of the adversary's intelligence system for answers to specific questions about friendly intentions, capabilities, limitations, and activities will be part of critical information.

(2) The next higher echelon publishes OPSEC guidance for subordinate units to support its OPSEC program. Subordinate units develop their critical information at the lowest level and forward their CIL to higher echelons. Higher echelons consolidate lower echelons' critical information as a foundation for their own CIL. Final CILs from higher echelons are then sent down to subordinate units, which subordinate units must support.

(3) The commander, director, or equivalent leadership position will provide specific guidance.

(4) The security classification guide for a program or operation identifies classified critical information. The security classification guide itself identifies the most sensitive areas of an activity, program, project, or operation.

(5) Various laws and EOs require CUI to be protected. The following list contains examples of CUI, but is not all inclusive:

(a) Information concerning a protected person.

(b) Export-controlled technical data (on the Military Critical Technologies List, as required by the Export Administration Act (50 USC App. 2401–2420), extended by EO 13222 under the International Emergency Economic Powers Act (50 USC 1701–1707)).

(c) Critical information.

(d) Contract financial data in the pre-award stage.

(e) Military operational and tactical information.

(f) DoD-developed computer software.

(g) Proprietary data (trade secrets).

(h) Test materials used in an academic environment.

(i) Law enforcement sensitive information.

(j) Personally identifiable information.

(6) Associations. Appendix C has sample critical information by category of information.

(7) Indicators that would reveal critical information are also critical information. Appendix D has samples of OPSEC indicators that could reveal critical information.

(a) Identify the length of time critical information needs protection. Not all information needs protection for the duration of an operation.

(b) The commander must approve the organization's critical information and abide by critical information provided.

### **B-3. Analysis of Threats**

a. Purpose. The purpose of this step is to identify adversary collection capabilities against critical information. Adversary collection activities target actions and open source information to obtain and exploit indicators that will negatively impact the mission. OPSEC indicators are friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information (see appendix D for sample OPSEC indicators).

b. Methodology.

(1) In coordination with the intelligence staff and all other staff elements, examine each part of the activity/operation to find actions or information that will provide indicators in each area (personnel, logistics, communications, movement activities, aviation, and so forth).

(2) Compare the identified indicators with the adversary's intelligence collection capabilities. A vulnerability exists when the adversary can collect an indicator of critical information, correctly analyze the information, make a decision, and take timely action to adversely influence, degrade, or prevent friendly operations. One method to use is to develop a "mission timeline." Identify along the timeline anything the commander has stated he or she wants protected.

(3) Have each staff element/participant in the action/operation identify along the "timeline," actions that "must be accomplished" in order for the mission to be accomplished.

(4) Identify which of these "must be accomplished" actions will be indicators an adversary could use. Now, compare each indicator with each of the adversary's collection capabilities. Where there is a match, there is a vulnerability. Consider the following questions:

(a) What critical information does the adversary already know? Is it too late to protect information already known by an adversary?

(b) What OPSEC indicators will friendly activities create about the critical information not already known by the adversary?

(c) What indicators can the adversary actually collect (this depends on the capabilities of the adversary's intelligence system)?

(d) What indicators will the adversary be able to use to the disadvantage of friendly forces?

(e) Which indicators can be used to friendly advantage by fostering a desired perception by the adversary that will be beneficial to friendly operations?

#### **B-4. Analysis of Vulnerabilities**

The purpose of this step is to identify each vulnerability and draft tentative OPSEC measures addressing those vulnerabilities. The most desirable measures provide needed protection at the least cost to operational effectiveness and efficiency.

a. OPSEC measures are methods and means to gain and maintain essential secrecy about critical information. There are three categories of measures to accomplish this.

(1) Action control consists of measures to control friendly activities. Action control can eliminate or reduce indicators or the vulnerability of actions to exploitation by adversary intelligence systems to an acceptable level. Select what actions to undertake, decide whether or not to execute

actions, or impose restraints on actions (trash control, mandatory use of secure communications, OPSEC reviews, and so forth) Specify who, when, where, and how.

(2) Countermeasures disrupt the adversary's information gathering or prevent their recognition of indicators when collected materials are processed. Use diversions, camouflage, concealment, jamming, deterrence, police powers, and force against adversary information gathering and processing capabilities.

(3) Counter-analysis is directed at the adversary analyst to prevent accurate interpretations of indicators during adversary analysis of collected material. Confuse the adversary analyst through deception techniques, such as cover.

b. Select at least one tentative OPSEC measure for each identified vulnerability. Some measures may apply to more than one vulnerability. Specify who, when, where, how, and for how long the measure is to be in effect.

c. Assess the sufficiency of routine security measures (personnel, physical, cryptographic, document, special access, automated information systems, and so on). These will provide OPSEC measures for some vulnerabilities.

d. If required, refer to AR 525–21(C) for information on deception, and refer to AR 381–102 (S) for information on cover.

e. Appendix F has sample OPSEC measures.

#### **B-5. Assessment of Risk**

The purpose of this step is to select which of the tentative OPSEC measures to implement. The OPSEC PM/officer recommends to the commander the OPSEC measures that he or she believes should be implemented, but the commander responsible for the mission must make this decision. The commander must balance the risk of operational failure against the cost of OPSEC measures.

a. Consider the following questions for each tentative measure. The PM/officer must be prepared to answer each of these questions for the commander.

(1) What is the likely impact of an OPSEC measure on operational effectiveness, if implemented?

(2) What is the probable risk to mission success (effectiveness), if the unit does not implement an OPSEC measure?

(3) What is the probable risk to mission success, if an OPSEC measure does not work?

(4) What is the impact on future missions if this measure is adopted and successful?

(5) What is the impact to other units of practicing an OPSEC measure?

b. Decide which, if any, OPSEC measures to recommend for implementation and when to do so.

c. Check the interaction of OPSEC measures. Ensure that a measure to protect a specific piece of critical information does not unwittingly provide an indicator of another.

- d. Determine the coordination requirements for OPSEC measures with the other capabilities.
- e. Submit the final selected OPSEC measures to the commander for approval.

f. The commander may decide on a no-measures alternative. This is acceptable, if the OPSEC process was used to determine that no critical information requires protection or that the costs outweigh the risks. However, that decision must be documented for future reference.

## **B-6 Application of Appropriate Operations Security Measures**

a. The purpose of this step is to apply OPSEC measures, approved by the commander, to ongoing activities or to incorporate them into plans for future operations. There are two aspects to this step—the PM/officer implements the OPSEC measures and then, unit personnel implement the OPSEC measures.

(1) The PM/officer implements OPSEC measures. The OPSEC officer can implement OPSEC measures by generating guidance or tasking. The guidance or tasking can be in the form of annexes to plans, OPSEC plans, SOPs, and memoranda which may be issued in hard copy or by electronically-transmitted messages. The OPSEC officer will—

(a) Incorporate OPSEC measures in the operation, activity, acquisition program, or project. Under the commander's authority, direct the implementation of those measures that require immediate action. This applies to current operations as well as planning and preparation for future ones.

(b) Document the OPSEC measures. Operations, exercises, RDT&E programs, acquisition programs, and other activities of interest to adversary intelligence services will have an OPSEC annex or plan (If the commander selected a no-measures alternative, state that fact).

(d) There is no set format for an OPSEC plan. Figure M-1 in AR 530-1 has a model outline of an OPSEC plan for activities, programs, or projects not documented by an OPORD or OPLAN. This model can apply to special access programs or acquisition systems program protection plans. Tailor the format and content of the OPSEC plan to meet the specific need. As a minimum, address the following points:

- Requirements for the identification and protection of critical information from initial planning through post execution phases.
- Tasks to staff and subordinate commands to plan and execute OPSEC measures.
- An OPSEC estimate comprising the identified or assumed adversary knowledge of friendly operations or activity, friendly critical information, and an evaluation of friendly OPSEC effectiveness.
- Intelligence collection threat consisting of friendly detectable indicators, critical information, and the adversary's capability to obtain and use the information.
- OPSEC measures to implement.

(e) Brief OPSEC requirements to planners, participants, and support personnel. OPSEC measures are command directed actions executed by individuals, who must be aware of their

responsibilities. Emphasize the adverse results of a failure to maintain effective OPSEC, particularly for long-term undertakings, such as RDT&E programs.

(2) Personnel within the organization execute OPSEC measures. The role unit personnel play begins upon receipt of the OPSEC guidance or tasking. By complying with the published OPSEC guidance or tasking, unit personnel functionally implement the required OPSEC measures.

b. After the implementation of appropriate measures, the OPSEC PM/officer should evaluate the effectiveness of OPSEC measures during execution.

(1) The application of OPSEC measures is a continuous cycle that includes evaluating intelligence and counterintelligence reports, public media disclosures, Web site reviews, integrated systems security monitoring, and feedback reports on OPSEC measures. Such reports include OPSEC assessments and surveys.

(2) As part of the OPSEC evaluation process, the OPSEC program manager/officer will—

(a) Evaluate the effectiveness of current OPSEC measures.

(b) Provide emphasis when needed.

(c) Recommend adjustments to improve the effectiveness of existing measures.

(d) Recommend new measures, if significant new vulnerabilities develop.

## **B-7. Planning Guidance**

a. OPSEC steps occur within the military decision making process. The OPSEC officer provides planning guidance for staff elements. Each staff element will identify the critical information, who is responsible for protecting it, and the vulnerabilities in their functional areas, and provide them to the OPSEC officer.

b. OPSEC planning guidance (provided as an OPSEC estimate) includes the following items:

(1) An estimate of probable adversary knowledge of the activity or operation.

(2) A preliminary list of critical information.

(3) A summary of adversary intelligence collection capabilities.

(4) A list of OPSEC indicators by staff function.

(5) A list of OPSEC measures to implement immediately and additional measures to consider.

c. By incorporating OPSEC into planning early on, the activity or operation will be more effective during execution.

d. For example, a unit may decide its upcoming deployment date is critical information. Critical information is revealed by visible indicators (for example, the inoculations that often take place prior to deployment). These indicators can be detected by an adversary based on the assessed threat. Since virtually any adversary can observe a unit gathering for inoculations, the threat is legitimate in

this case, and this is a vulnerability. To counter this vulnerability, the unit may direct an OPSEC measure, such as sending unit members in smaller groups for their inoculations. The OPSEC PM/officer would then observe and gauge the effectiveness of this measure and revise as appropriate.

## **Appendix C**

### **Sample Critical Information**

The following paragraphs provide a few examples of critical information. There are many other items of critical information 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 critical information unique to itself. To view the 8A CIL, refer to 8A Command Policy Letter #2 (OPSEC).

#### **C-1. Courses of Action**

- a. Specific courses of action (COA) the U.S. and allied commands are planning.
- b. Specific COA that U.S. and allied forces cannot undertake or execute.

#### **C-2. Forces**

- a. U.S. and allied forces earmarked for possible COA.
- b. Readiness levels of organizations.
- c. Specific current force/unit locations.
- d. Specific projected force/unit locations.

#### **C-3. Mission Command**

- a. U.S. and allied command arrangements for executing COA.
- b. Current or future locations of unit commanders.
- c. Current or future command post locations.
- d. Command post vulnerabilities.

#### **C-4. Communications**

- a. Command, control, communications, computers, and intelligence capabilities.
- b. Communications sites locations.
- c. Communications limitations (weather, terrain and equipment shortages, and so forth).

#### **C-5. Logistics**

- a. Logistical posture of U.S. and allied forces.
- b. Speed of deployment/redeployment of ground and air forces.
- c. Pertinent ground, air, and sea lines of communications; locations of storage depots, ports, and airfields.
- d. Vulnerabilities to interdiction of the lines of communication.
- e. Contents of Army prepositioned stocks and significant restructuring of Army prepositioned stocks.

#### **C-6. Supplies**

- a. Levels of supplies available for immediate support.
- b. Pre-positioned supply sites.
- c. Period of combat sustainment with those supplies.
- d. Critical item shortages (in all classes).
- e. Limitations to resupply capability.
- f. Demand level for Class IX items.

#### **C-7. Locations**

- a. Specific locations of exercises and operations.
- b. Specific locations of participating forces.
- c. Specific projected force/unit locations.
- d. Alternate force/unit locations.

**C-8. Vulnerabilities**

- a. Vulnerabilities of defensive dispositions.
- b. Vulnerabilities of sensors and other capabilities to detect attack.
- c. Vulnerabilities to attack.
- d. Vulnerabilities of units and weapons and weapons systems.
- e. Vulnerabilities in protection or security forces or security plans.

**C-9. Intelligence**

- a. Intelligence, surveillance, and reconnaissance (ISR) resources available to support the commander.
- b. Locations of those ISR capabilities.
- c. Ongoing ISR operations and their goals.
- d. Vulnerabilities to exploitation or destruction of those friendly ISR capabilities.

**C-10. Rules of Engagement.** Policies and rules of engagement that govern the use of weapons and electronic or acoustic warfare systems.

**C-11. Allies**

- a. Nations providing current or future support to the United States.
- b. Vulnerabilities that could be exploited to reduce or eliminate such support.

**C-12. Maintenance**

- a. Maintenance and salvage capabilities of the United States and allied forces.
- b. To what degree these capabilities can support and sustain forces in combat.
- c. Vulnerabilities to attack.

**C-13. Weapons**

- a. Specific characteristics and capabilities of weapons and electronic systems available to coalition forces.
- b. Doctrine for using various weapons.
- c. Indicators that unconventional weapons will be employed.
- d. New weapons that are available or are being employed.
- e. Vulnerabilities and limitations in friendly weapons and weapons systems.

**C-14. Military Information Support Operations**

- a. Intended psychological warfare and subversion operations.
- b. Plans to exploit adversary vulnerabilities.
- c. Ongoing operations.
- d. U.S. agencies conducting operations.
- e. Military information support operations themes and objectives.
- f. Vulnerabilities of U.S. forces to psychological warfare and subversion.

**C-15. Special Operations Forces and Unconventional Warfare**

- a. Intended sabotage and direct action mission targets.
- b. Adversary vulnerabilities planned for exploitation.
- c. Friendly capabilities to conduct unconventional warfare operations.
- d. U.S. agencies controlling those resources.
- e. Special operations forces (SOF) team deployment dates.
- f. SOF team deployment sites.
- g. Number of SOF teams/personnel in an area.
- h. Indigenous support to SOF teams.
- i. Conventional units associated with SOF teams/personnel.

**C-16. Deception**

- a. Planned political and military deceptions.
- b. Ongoing deception operations.
- c. U.S. agencies conducting deception operations.
- d. Identity of military units/organization conducting or participating in deception activities.

**C-17. Counterintelligence**

- a. U.S. counterintelligence capabilities to detect and neutralize espionage and sabotage nets.
- b. Number of CI assets available.
- c. Identification and location of CI elements and activities.
- d. Identification of local personnel that may be assisting friendly CI forces.

**C-18. Medical**

- a. Casualty figures, both actual and projected.
- b. Very Important Persons (VIP) being treated by our medical treatment facilities.
- c. Overall bed/treatment capacity.
- d. Increased medical supplies (vaccines, blood products, and so forth) required by unit or theater.
- e. Shortages in medical military occupational specialties and personnel.
- f. Identification of projected medical personnel/team deployments.
- g. Specific identification of classified medical-related research programs.
- h. Identified medical vulnerabilities of friendly forces.

**C-19. Government Contractors**

- a. Programs in which the contractor provides classified services and support to the U.S. Government.
- b. Pre-contract award identification of locations of contractor duty.
- c. Contractor increasing hiring for new or existing contracts or programs.
- d. Contractor information or service-sharing agreements with other private organizations.

**C-20. Arms Control Treaty Inspections**

- a. Missions of the activities on the installations to be visited.
- b. If the installation to be visited is self-sufficient or reliant on the local community for support (that is, telephone service, electricity, water, fire department, police, and so forth).
- c. If all the buildings on the installation are in use.
- d. Access to the post.
- e. Morale of installation personnel.
- f. Condition of the installation.
- g. Portions of the installation that appear to have more protection/security than other parts of the installation.
- h. Security procedures in place at this installation (Federal Bureau of Investigation support, physical security, counterintelligence activities, law enforcement).

**C-21. Special Access Programs**

- a. Organizations and contractors involved in the SAP.
- b. Mission or subject of the SAP.
- c. Operational life of the SAP/current stage of development.
- d. Security procedures for the SAP.
- e. Budget for the SAP.
- f. Number of personnel in the SAP.
- g. Existence and identification of an unacknowledged SAP.

**C-27. Cyberspace**

- a. Wireless communication.
- b. Computer network defense.

## Appendix D Operations Security Indicators

### D-1. Characteristics

Indicators are 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 capabilities, activities, limitations, and intentions. An item which meets any of the characteristics below (signature, association, profile, contrast, or exposure) is an indicator. Indicators are the bits and pieces of information and data that the adversary analyst pieces together to develop his intelligence estimate. Indicators are what the adversary uses to formulate his perception of our operations. To view 8A OPSEC indicators, refer to 8A Command Policy Letter #20 (OPSEC).

We can manage the adversary's perception by managing the indicators. OPSEC 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. An example is the unique design of the M-1-series main battle tank. Its visual signature cannot be mistaken from most tanks. A unique visual signature minimizes 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. These features 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. The presence of special operations aviation aircraft, such as the MH-6, MH-60, and MH-47, may be indicators of other SOF operating in the area. Certain items of equipment that are particular to specific units are indicators of the potential presence of related equipment. For example, the sighting of an M-88A2 Hercules Recovery Vehicle likely indicates the presence of an armored unit equipped with M1A2-series tanks, as the M-88A2 is rated to recover and tow the M1A2-series tanks. Such continuity can result from repetitive practices or sequencing instead of from planned procedures. When detecting some components of symmetrically-arrayed organizations, the adversary can assume the existence of the rest. As another example, the adversary would suspect the presence of an entire infantry battalion, when intelligence detects 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.* Each functional activity has a profile made up of unique indicators, patterns, and associations. The profile of an aircraft deployment, for example, may be unique to the aircraft type or mission, as in the special operations aviation example. 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 appear to 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. In the special operations aviation example, if the adversary identifies items unique to special operations aviation at an airfield, this will contrast with what is "normal" at the airfield and will indicate the deployment of special operations aircraft to the airfield without having actually observed them.

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 into the background of insignificant anomalies. Repetition is the most dangerous. Operations conducted the same way several times with little or no variation provide an adversary the information needed to determine where, when, how, and with what to attack. This is a lesson learned at the cost of many lives during every war.

## **D-2. Sample Operations Security Indicators**

The following are 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. To view 8A OPSEC indicators, refer to 8A Command Policy Letter #20 (OPSEC).

## **D-3. Administration**

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

## **D-4. Operations, Plans, and Training**

- a. Changes in defense readiness condition, force protection condition, or information condition.
- 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. Repeating operations the same way, same time, same route, or in same area. Fixed schedules and routes.
- h. Standard reactions to hostile acts.
- i. Standardizing maneuvers or procedures.
- j. Standardizing force mixes and numbers to execute particular missions down to squad-level operations.

- k. Changing guards at fixed times.
- l. Appearance of special purpose units (bridge companies, pathfinders, explosive ordnance detachments, SOF, liaison officer teams, and so forth).
- m. Change in task organization or arrival of new attachments.
- n. Artillery registration in new objective area.
- o. Surge in food deliveries to planning staffs at major headquarters.
- p. Unit and equipment deployments from normal bases.

#### **D-5. Communications**

- a. Voice and data (telephone, cellular phone, wireless) transmissions between participants in an operation.
- b. Establishment of command nets.
- c. Changes in message volume (phone calls to secure systems), such as increased radio, e-mail, and telephone traffic from headquarters.
- d. Units reporting to new commanders.
- e. Identification of units, tasks, or locations in unsecured transmissions.
- f. Increased communications checks between units/organizations.
- g. Unnecessary or unusual increase in reporting requirements.
- h. Sudden imposition of communications security measures, such as radio silence.
- i. Appearance of new radio stations in a net.
- j. Communications exercises.
- k. Appearance of different cryptographic equipment or materials.
- l. Increase in unofficial use of commercial e-mail services.
- m. Unofficial use of instant messenger and chat forums.
- n. Increased FRG/FRSA posture.

#### **D-6. 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. Increased ground patrols.
- h. Unusual or increased requests for meteorological or oceanographic information.
- i. Unique or highly visible security to load or guard special munitions or equipment.
- j. Adversary radar, sonar, or visual detection of friendly units.
- k. Friendly unit identifications through communications security violation, physical observation of unit symbols, and so forth.
- l. Trash and recycle bins that contain critical information.

#### **D-7. Logistics**

- a. Volume and priority of requisitions.
- b. Package or container labels that show the name of an operation, program, or unit designation.
- c. Prepositioning 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. Stockpiling petroleum, oil, lubricants, and ammunition.
- l. Upgraded lines of communication.
- m. Delivery of special or uncommon munitions.
- n. New support contracts or host nation agreements.
- o. Arranging for transportation and delivery support.
- p. Requisitions in unusual quantities to be filled by a particular date.

**D-8. Engineer**

- a. New facility leases.
- b. Construction of mock-ups for special training.
- c. Production or requisitions of unusual amounts of maps and charts or products for unusual areas.
- d. Attachment of specialized heavy equipment.

**D-9. Medical**

- a. Stockpiling plasma and medical supplies.
- b. Movement of deployable medical sets.
- c. Immunization of units with area-specific and time-dependent vaccines.
- d. Identifying special medical personnel and teams deploying to specific areas.
- e. Sudden recall of Army National Guard and Army Reserve doctors to active duty.

**D-10. Emissions Other than Communications**

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

**D-11. Research, Development, Test and Evaluation and Acquisition Activities**

- a. Solicitations for subcontractors to perform portions of the work.
- b. Lists of installations that are involved in particular contracts or projects.
- c. Specialized hiring of personnel for particular contracts or projects.
- d. Highlighting specific security needs or requirements for portions of a projector contract.
- e. Testing range schedules.
- f. Unencrypted emissions during tests and exercises.
- g. Public media, particularly technical journals.
- h. Budget data that provides insight into the objectives and scope of a system research and development effort or the sustainability of a fielded system.
- i. Deployment of unique units, targets, and sensor systems to support tests associated with particular equipment or systems.
- j. Unusual or visible security imposed on particular development efforts that highlight their significance.
- k. Special manning for tests or assembly of personnel with special skills from manufacturers known to be working on a particular contract.
- l. Stereotyped use of location, procedures, and sequences of actions when preparing for and executing test activity for specific types of equipment or systems.
- m. Advertisements indicating that a company has a contract on a classified system or component of a system, possesses technology of military significance, or has applied particular principles of physics and specific technologies to sensors and the guidance components of weapons.

- n. Schedules (delivery, personnel arrival, transportation, test, ordnance loading, and so forth) posted where personnel without a need-to-know have access.
- o. Conferences, symposia, and internal professional forums.

## **Appendix E**

### **The Threat**

#### **E-1. Summary**

Because the U.S. military is superior in traditional forms of warfare, adversaries and potential adversaries have shifted away from traditional warfare and have adopted asymmetric methods and means. In addition to traditional capabilities and methods, adversaries also will conduct irregular, catastrophic, and disruptive forms of warfare.

#### **E-2. Adversaries**

- a. Non-state actors.
- b. Nation-states.
- c. Domestic threats.
- d. Criminals.
- e. Hackers.
- f. Insiders.

#### **E-3. Threat Collection in the Basic Intelligence Disciplines**

- a. All-source intelligence
- b. Human intelligence
- c. Imagery intelligence
- d. Signals intelligence
- e. Measurement and signature intelligence
- f. Technical intelligence
- g. Counterintelligence.

## **Appendix F**

### **Sample Operations Security Measures**

The OPSEC measures in this appendix are only examples to stimulate thought. Do not use them as a checklist. This is not a comprehensive list. Possible OPSEC measures are as varied as the specific vulnerabilities they address. To view 8A OPSEC measures, refer to 8A Command Policy Letter #20 (OPSEC).

#### **F-1. Operations and logistics**

- a. Randomize the performance of functions and operational missions. Avoid repetitive or stereotyped tactics and procedures for executing operations or activities in terms of time, place, event sequencing, formations, and mission command arrangements.
- b. Employ force dispositions and mission command arrangements that conceal the location, identity, and command relationships of major units.
- c. Conduct support activities in a way that will not reveal intensification of preparations before initiating operations.
- d. Transport supplies and personnel to combat units in a way that conceals the location and identity of the combat units.
- e. Operate aircraft at varying altitudes, and use random flight routes.
- f. Operate to minimize the reflective surfaces that units and weapon systems present to radar and sonar.
- g. Use darkness to mask deployments or force generation.
- h. Approach an objective "out of the sun" to prevent detection.
- i. Randomize convoy routes, departure times, speeds, and so forth.
- j. Do not set patterns to patrolling activities (start times, locations, number of personnel in a patrol, and so forth).
- k. Do not use same landing zone or pick-up point repetitively.
- l. Do not use same approach (aircraft) or route (vehicle) into and out of an area repetitively.
- m. Do not establish overwatch, sniper, communications, and medical evacuation/support positions at the same location every time out.
- n. Vary small unit patrol formations; do not set patterns.

#### **F-2. Technical**

- a. Use radio communications emission control, low probability of intercept techniques, traffic flow security, ultra-high frequency relay via aircraft, burst transmission technologies, secure phones, landline, and couriers. Limit use of high frequency radios and directional super high frequency transponders.
- b. Control radar emissions and operate at reduced power.
- c. Mask emissions of forces from radar or visual detection by use of terrain (such as hills and mountains).
- d. Maintain noise discipline, operate at reduced power, proceed at slow speeds, and turn off selected equipment.
- e. Use camouflage, smoke, background noise, added sources of heat or light, paint, or weather.
- f. Use deceptive radio transmissions.
- g. Use decoy radio or emission sites.

#### **F-3. Administrative**

- a. Avoid bulletin board plan of the day or planning schedule notices that reveal when events will occur.
- b. Conceal budgetary transactions, supply requests and actions, and arrangements for services that reveal preparations for activity.
- c. Conceal the issuance of orders, the movement of specially-qualified personnel to units, and the installation of special capabilities.

*d.* Control trash dumping or other housekeeping functions to conceal the locations and identities of units.

*e.* Destroy (burn, shred, and so forth) paper to include unclassified information to prevent the inadvertent disposal of classified and sensitive information.

*f.* Follow normal leave and pass policies to the maximum extent possible before an operation starts in order to preserve an illusion of normalcy.

*g.* Ensure personnel discreetly prepare for their Family's welfare in their absence, and their Families are sensitized to their potential abrupt departure.

*h.* Maximize use of security screening of local national hires and minimize their access and observation opportunities.

*i.* Randomize security in and around installation/camp to prevent setting a pattern or an observable routine.

*j.* Conduct random internal (in camp) unannounced identity and security inspections.

#### **F-4. Military Deception**

*a.* MILDEC can directly support OPSEC by distracting foreign intelligence away from, or provide cover for, military operations and supporting activities. MILDEC can be planned and executed by, and in support of, all levels of command to support the prevention of an inadvertent compromise of classified information, critical information, and sensitive unclassified information. OPSEC and MILDEC must be synchronized and deconflicted to ensure that MILDEC is effective and believable.

*b.* OPSEC can also support MILDEC. An OPSEC analysis of a planned activity or operation identifies potential OPSEC vulnerabilities. Those vulnerabilities are useful to MILDEC planners as possible conduits for passing deceptive information to an adversary. Additionally, MILDEC actions often require specific OPSEC protection. An OPSEC analysis of a planned MILDEC is needed to protect against an inadvertent or unintentional outcome. Failure to maintain good OPSEC can lead to identification of the operation as a deception effort and cause the adversary's intelligence services to refocus their attention on the actual friendly operation.

#### **F-5. Combat Action**

During hostilities, use force against the adversary's ability to collect and process information. This can involve interdiction, sabotage, direct action missions, guerrilla operations, or strikes against adversary targets.

## **Appendix G**

### **Operations and Security Relationships to Security Programs**

#### **G–1. Background**

As stated in chapter 1 of this regulation, OPSEC protects critical information from adversary observation and collection in ways traditional security programs cannot. While security programs focus on protecting classified information, OPSEC focuses on eliminating, reducing, or concealing the unclassified indicators that can compromise classified information, especially critical information. Despite these differences, OPSEC and security programs are related and must be mutually supporting in order to ensure maximum protection of classified information as well as critical information. The following paragraphs address the relationship of OPSEC to other programs.

#### **G–2. Information Security**

a. INFOSEC is the system of policies, procedures, and requirements established under the authority of EO 13526, to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

b. AR 380–5 provides guidance for classifying material to prescribe the level of protection afforded to it. Protective measures (such as security containers) deny unauthorized personnel access to classified material. The threat of open source exploitation and possible non-compliance with procedures intended to keep classified material from appearing in open sources are OPSEC concerns.

c. Bits of information conveyed in non-secure radio transmissions, non-secure telephone calls, unencrypted e-mail containing sensitive information, public releases, briefings for the public, friendly conversations in public areas, and so forth, permit adversaries to piece together U.S. intentions and military capabilities. Implementation of OPSEC measures prevents critical information from appearing in open sources.

#### **G–3. Information Assurance**

a. IA is the protection of information systems and information in storage, processing, or transit from unauthorized access or modification; 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. See AR 25–1 and AR 25–2 for more information.

b. IA provides the means to ensure the confidentiality, integrity, and availability of information processed by the Army's information-based systems. It provides a measure of confidence that the security features, practices, procedures, and architectures of an information system accurately mediates and enforces the security policy. IA supports OPSEC by ensuring the confidentiality of information when it is transmitted from the sender to the recipient(s). Confidentiality is the assurance that information is not disclosed to unauthorized entities or processes.

c. IA is the security discipline that encompasses communications security (COMSEC), computer security, and emanations security. See AR 380–40, AR 380–27, and AR 25–2.

(1) Communications security consists of measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. COMSEC is of particular interest to OPSEC. The intercept of non-secure communications is a significant source of intelligence information and OPSEC indicators for adversaries. Components of COMSEC are cryptographic and transmission security.

(a) Cryptographic security is the use of encryption systems to transmit information by message or telephone, which is encrypted or sent using an authorized code. OPSEC is concerned with any deviation from established cryptographic practices that would permit any adversary to "read" U.S. message traffic. OPSEC is also concerned with the possible release of specific information about how friendly cryptographic systems are used or any vulnerabilities that may exist.

(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 a communications signal, the intercept of a signal (such as, deviation of location or identity) and the patterns and volumes of communications from and to various locations. All of these may be OPSEC indicators.

(2) Computer security consists of measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer or AIS. Computer security prevents the intentional or accidental penetration of an AIS. It avoids the disclosure, modification, or destruction of AIS and associated data. Examples are "hacker" penetrations and computer "virus attacks."

(3) Emanations security is the component of COMSEC that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems. In emissions security, TEMPEST refers to investigations and studies of compromising emanations.

#### **G-4. Electronic Security**

Electronic security (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. Reducing the information content of the emitters to make them more difficult to identify and locate is ELSEC and is also an OPSEC measure.

#### **G-5. Emanation Control**

Emanation control is the selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities, while minimizing, for OPSEC—

- a. Detection by enemy sensors.
- b. Mutual interference among friendly systems.
- c. Enemy interference with the ability to execute a MILDEC plan.

#### **G-6. Military Deception**

MILDEC supports military operations through the application of techniques that simultaneously deny certain true information or indicators and convey or display false information or indicators that will be accepted by adversaries. MILDEC actions mislead adversaries, causing them to derive and accept desired appreciations of U.S. military capabilities, intentions, operations, and other activities.

a. Depending on the objective, MILDEC can be an OPSEC measure, or OPSEC can support MILDEC. When procedural or physical security means are unavailable for controlling OPSEC vulnerabilities, MILDEC can mislead adversaries, thereby minimizing the OPSEC vulnerability.

b. OPSEC supports MILDEC planners by assisting in determining the indicators that the adversary should be allowed to see in order to make the deception appear believable and determining which indicators of a deception that must be protected and how to protect them.

### **G-7. Physical security**

Physical security consists of protective measures to deny unauthorized personnel access to specific areas, facilities, material, or classified information.

a. By denying access, physical security measures can be an OPSEC measure. However, physical security measures can become compromised (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).

b. OPSEC can support physical security by identifying those actions and information that would be indicators an adversary could exploit.

### **G-8. Force Protection**

Force protection consists of actions taken to prevent or mitigate hostile actions against all DoD personnel (Service members, 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. OPSEC plays a vital role in the following ways:

a. OPSEC can identify indicators of routine actions observable by a terrorist that represent a vulnerability both in a tactical environment and in garrison.

b. OPSEC can assist in determining measures to negate effective terrorist collection of information needed for planning.

c. OPSEC can identify indicators and recommend OPSEC measures to protect possible or existing vulnerabilities in protective measures.

d. OPSEC can assist traditional security disciplines in ensuring their protective measures are in the right place at the right time.

e. OPSEC develops critical information that identifies what must not be allowed to appear in the public domain to prevent collection by a terrorist.

### **G-9. Program Protection Planning (PPP)**

a. DoDI 5200.39 identifies the requirements for PPP. This directive specifies CPI (the focus of program protection planning) shall be identified early in the acquisition life cycle, but not later than Milestone B, or when the program enters the acquisition process. It also states that, if CPI is identified, then a PPP is required. DoDI 5200.39 does not allow for waivers or exceptions to this requirement. If no CPI is identified, a PPP is not required.

b. DoDI 5200.39 references DoDM 5200.01 as a procedural manual for the development and implementation of PPPs. The PPP uses security disciplines and OPSEC to achieve protection.

## **Appendix H Standard Duty Description for Operations Security Program Managers, Officers, and Coordinators**

### **H-1. Overview**

This section discusses the three positions of the OPSEC program.

### **H-2. General Operations Security Duties**

- a. Organize and manage the unit, activity, installation, or organization's OPSEC program to include subordinate OPSEC programs.
- b. Identify the organization's critical information, recommend the CIL to the commander for approval, and publish the CIL.
- c. Publish an OPSEC SOP/plan per guidance of this regulation. Ensure the OPSEC SOP/plan conforms to guidance from higher headquarters and any applicable local authorities, such as the installation OPSEC PM.
- d. Maintain awareness of all unit activities and advise appropriate personnel about the organization's OPSEC posture and offer recommendations to eliminate or reduce vulnerabilities.
- e. Conduct OPSEC reviews per guidance of this regulation.

### **H-3. Operations Security Program Manager Duties**

The organization's OPSEC PM administers the commander's OPSEC program. An OPSEC PM is responsible for the development, organization, and administration of an OPSEC program at ACOM, ASCC, DRU, garrison, and corps and higher. The OPSEC PM 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 PMs are also OPSEC officers, but because of the extent and complexity of the OPSEC program they oversee, they are primarily referred to as OPSEC PMs. In addition to H-2, above, OPSEC PMs —

- a. Integrate, coordinate, and synchronize subordinate OPSEC programs.
- b. Coordinate with the Army OSE prior to conducting OPSEC Level II training.
- c. Oversee all OPSEC training requirements.
- d. Establish OPSEC as an element of the CIP.
- e. Conduct OPSEC assessments of their own organization and subordinate elements.
- f. Interface with all subordinate OPSEC officers and coordinators on issues that affect the command.
- g. Interface and conduct OPSEC coordination with all higher headquarters.
- h. For ACOMs, ASCCs, and DRUs, submit the annual OPSEC report to the Army OPSEC PM.
- i. Maintain contact with Army protection personnel and security agencies to obtain information that supports the OPSEC planning process.

*j.* Ensure OPSEC is included in planning for future operations, exercises, tests, and activities. As required, write OPSEC documents, annexes, and appendices to OPLANSs and OPORDs. Write OPSEC documents as required for activities not covered by OPLANS and OPORDs.

*k.* Organize and provide oversight to an OPSEC working group. An OPSEC working group brings together OPSEC officers and other security-related positions to ensure the OPSEC program is consistent across the organization and is integrated at the work level. The working group will assist the OPSEC PM in developing OPSEC measures and solutions to implementation problems. The working group will provide coordination of all recommendations being forwarded to senior leadership and will assist with development of briefings and reports.

*l.* Interface with acquisition managers so that OPSEC is addressed throughout the lifecycle of any acquisition program.

#### **H-4. Operations security officer duties**

The OPSEC officer is responsible for the development, organization, and administration of an OPSEC program at division-level and below. In addition to H-2, above OPSEC officers—

- a.* Conduct the command's OPSEC Level I training.
- b.* Maintain contact and coordination with the next higher echelon OPSEC officer or OPSEC PM.
- c.* Where appropriate and as required, conduct OPSEC assessments of their own organization and of subordinate units.
- d.* As required, write OPSEC documents, annexes, and appendices to OPLANS and OPORDs. Write OPSEC SOPs/plans as required for activities not covered by OPLANS and OPORDs.
- e.* For OPSEC officers in RDT&E activities, provide specific and tailored OPSEC guidance to activities that are involved in developing system requirements and to associated system development, tests, and evaluations.

#### **H-5. Operations security coordinator duties**

The OPSEC coordinator has a significant role in the OPSEC program. The OPSEC coordinator assists the OPSEC PM or OPSEC officer in the development, organization, and administration of the OPSEC program. The OPSEC coordinator may be uniformed personnel, a DA civilian employee, or a contractor. 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 PM or OPSEC officer. However, they may perform OPSEC duties in a supporting capacity as the OPSEC coordinator.

#### **H-6. Qualifications for operations security program manager/officer/coordinator**

- a. Experience and knowledge.*
  - (1) Operations experience is essential to the OPSEC PM, officer, and coordinator.
  - (2) The OPSEC PM, officer, or coordinator should have experience in planning and conducting information gathering activities, processing, and extracting data from materials gathered, the concept of indications and warnings, and problem-solving techniques. Ideally, they would have

experience in the intelligence process, including intelligence analysis and estimation techniques. This experience is secondary to operations experience.

(3) Thorough comprehension of the functional relationships and procedural processes of the unit or organization.

(4) Working knowledge of Army and command planning systems, directives, and the organization's plans and procedures.

(5) Basic knowledge of traditional security programs intended to protect classified information and matters and their distinct relationship to OPSEC.

*b. Training and education.*

(1) OPSEC PM is required to attain Level II certification and strongly recommended to attain Level III certification.

(2) OPSEC officer is required to attain Level II certification and is encouraged to attain Level III certification based on recommendation from chain of command and OPSEC program manager.

(3) OPSEC coordinator is required at a minimum to complete the IOSS OPSEC Fundamental Course (OPSE 1301) or equivalent. If executing duties as described in paragraphs H-3 or H-4, above, these individuals are now performing the duties of an OPSEC officer and will attend OPSEC Level II certification.

(4) Level II certification must be attained within 90 days of appointment.

*c. OPSEC skills.*

(1) Ability to provide advice about policies, doctrine, and guidance and apply effective OPSEC measures.

(2) Ability to integrate and coordinate OPSEC planning with the other capabilities of IO.

*d. Communicative skills.*

(1) Ability to independently develop and present clear, concise briefings with sound conclusions and recommendations.

(2) Ability to develop OPSEC awareness training programs and present them to all personnel.

(3) Ability to write and organize concise plans, directives, and training materials.

*e. Security clearance.* All OPSEC PMs, officers, and coordinators must be eligible to be cleared to the highest level of classified information and accesses required for them to provide OPSEC support to their command or organization. At a minimum, all personnel serving in an OPSEC duty position will have a SECRET clearance.

## **Appendix I Annual Operations Security Report Format**

### **I-1. Overview of Operations Security Program Status**

The annual OPSEC report is used to gather information throughout 8A on OPSEC programs. This information will be consolidated into a report to USARPAC and the OUSD (I) to provide a status on Army OPSEC programs. The purpose of this report is to identify Army OPSEC challenges and to chart a way ahead that feeds resourcing justifications and decisions. The OPSEC report is 8A's opportunity to shape USARPAC and Office of the Secretary of Defense resource decisions regarding OPSEC.

a. 8A MSCs will send a report to the 8A OPSEC PM at 8A ACoS G33. 8A MSCs will require annual OPSEC reports from subordinate units down to Battalion level. The annual OPSEC report is a bottom up generated reporting mechanism and it is imperative units at all levels submit timely reports to the next higher echelon.

b. The reporting period is from 1 October to 30 September of the prior fiscal year. The Army OPSEC PM will specify a suspense date via ALARACT message for ACOMs, ASCCs, and DRUs to submit their reports.

### **I-2. 8A MSC Operations Security Report Format**

In accordance with para I-2, AR 530-1, 8A MSCs will submit an annual OPSEC report in accordance with Figure I-1, 8A MSC Annual OPSEC Report Format, below.

- a. Unit commander's, or designated representative's, signature is required.
- b. Units will account for internal staffing timelines when ensuring final signed report is submitted on time.
- c. Units will submit a signed .pdf version of the document to the 8A OPSEC PM, 8A ACoS G33.
- d. Units will format the report in accordance with AR 25-50, Preparing and Managing Correspondence, 17 May 2013 (diagram below is for illustration purposes only and is not formatted in accordance with AR 25-50).



**DEPARTMENT OF THE ARMY**  
**HEADQUARTERS, EIGHTH ARMY**  
**UNIT #15236**  
**APO AP 96205-5236**

<OFFICE SYMBOL>

<DATE>

MEMORANDUM FOR OPSEC Program Manager, Eighth Army, United States Army Garrison –  
Yongsan, Republic of Korea 96205-5236

SUBJECT: FY <YEAR> Annual Operations Security Report

1. In accordance with appendix I, Army Regulation 530-1, Operations Security (OPSEC), 14 September 2014 and 8A OPOD XXX-XX, <UNIT> submits the Annual Operations Security report covering the period 1 October 2014 through 30 September 2015.

2. Program management. Provide a description of the command's OPSEC program management with the following details.

a. Indicate how many full-time and part-time personnel are assigned to your OPSEC program.

<INSERT RESPONSE>

b. Have you received OPSEC assistance from, or utilized the services of, the Army OSE or the IOSS?

<INSERT RESPONSE>

(1) If yes, what kind of support? (OPSEC assistance may include staff assistance, program development, planning, or training support.) If any requests were unfulfilled, please explain the circumstances.

<INSERT RESPONSE>

(2) What OPSEC training has the command's OPSEC program manager received?

<INSERT RESPONSE>

c. What does your organization do to make OPSEC a priority?

<INSERT RESPONSE>

3. Program plans and procedures. Summarize how well subordinate organizations are executing DOD and Army guidance on OPSEC planning and implementation with the following details.

a. List the OPSEC policies and planning guidance your organization has issued.

<INSERT RESPONSE>

b. Have you identified the critical information within your organization?

<INSERT RESPONSE>

c. How is that critical information communicated to the command's staff and personnel?

<INSERT RESPONSE>

d. How is the CIL kept up to date as missions change?

<INSERT RESPONSE>

e. Discuss the OPSEC measures that your command employs.

<INSERT RESPONSE>

f. Have you developed procedures and/or tools to assist with OPSEC implementation? If yes, please describe, and indicate whether this could be shared with other Army elements and DOD.

<INSERT RESPONSE>

g. Describe the procedures and protocols used to review open source material for critical and sensitive information.

<INSERT RESPONSE>

h. Describe the process to include OPSEC in the review of information prior to public release.

<INSERT RESPONSE>

4. Assessments. This section requests information on the command's OPSEC assessments, assessment findings and trends, and corrective actions. Please provide the following details.

a. Did you conduct an annual OPSEC assessment? Please describe the type of assessment performed. (Assessments may include self-assessments, assessments and/or surveys supported by the IOSS or Joint OSE, or another type of program review.)

<INSERT RESPONSE>

b. Did your command request assessment assistance from outside sources? If so, from which sources and for what support?

<INSERT RESPONSE>

c. What OPSEC trends and issues were identified by your assessment(s)? (Provide a summary, without unit specific information, on trends or issues which could indicate an Army-wide OPSEC issue.)

<INSERT RESPONSE>

5. OPSEC training and awareness. Provide an assessment of the command's OPSEC training and awareness programs with the following details.

a. Describe the command's OPSEC awareness program.

<INSERT RESPONSE>

b. Have you identified OPSEC training requirements commensurate with the respective responsibilities of OPSEC assigned personnel? Please describe (for example, training requirements for OPSEC program managers, planners, OPSEC coordinators, OPSEC working group, and so forth).

<INSERT RESPONSE>

6. Program resources. Summarize the command's investment in the OPSEC program with the following details:

a. Describe what resources you apply to your OPSEC program. (Applied resources might include awareness products, conference fees, mobile training teams, and so forth).

<INSERT RESPONSE>

b. Describe funding shortfalls in the command's OPSEC program.

<INSERT RESPONSE>

7. Miscellaneous problems and recommendations. Address problems, not previously addressed, that impact on the command's overall OPSEC posture. Such problems might include personnel manning or administrative problems.

<INSERT RESPONSE>

8. Forecast of OPSEC activities and objectives for the next reporting period. Address those planned actions that will improve the OPSEC posture of the command. These actions could involve new initiatives or refinement of OPSEC activities previously discussed.

<INSERT RESPONSE>

9. Pre- and post-deployment actions. How is OPSEC training provided in conjunction with pre- and post-deployment actions per AR 530-1 and AR 350-1? If not, why not?

<INSERT RESPONSE>

10. Trained personnel. How does your command ensure there are enough Level II trained personnel to meet your command's requirements?

<INSERT RESPONSE>

11. Provide a list of unit/organization public facing website addresses in accordance with enclosure 1.

12. Point of contact for this report is <RANK & NAME>, <DUTY POSITION>, at <ENTERPRISE EMAIL> or <DSN PHONE>. Alternate OPSEC PM is is <RANK & NAME>, <DUTY POSITION>, at <ENTERPRISE EMAIL> or <DSN PHONE>.

Encls  
A. Unit Public Facing Websites

<COMMANDER>  
<RANK>, <BRANCH>  
Commanding

---

**Figure I-1. 8A MSC Annual OPSEC Report Format**

---

**I-3. 8A Operations Security Report Format**

8A OPSEC PM will submit a consolidated 8A Annual OPSEC Report to USARPAC in accordance with figure I-2, 8A Annual OPSEC Report Format, below (completed example).



DEPARTMENT OF THE ARMY  
HEADQUARTERS, EIGHTH ARMY  
UNIT #16236  
APO AP 96205-5236

EACS-D

MEMORANDUM FOR Operations Security (OPSEC) Program Manager (PM),  
Headquarters, United States Army Pacific (USARPAC), Fort Shafter, Hawaii 96858-  
5100

SUBJECT: Fiscal Year (FY) 2015 Annual OPSEC Report

1. In accordance with Army Regulation (AR) 530-1, Operations Security (OPSEC), Appendix I and USARPAC Operations Order (OPORD) #16-11-022, Eighth Army (8A) submits the Annual OPSEC Report covering the period 1 October 2014 through 30 September 2015.

2. Program Management.

a. 8A has 111 part-time personnel assigned to our OPSEC program to include alternates. There are no full time personnel assigned to the program. There is one part-time Major assigned as the 8A OPSEC PM. Per Army in Korea (AK) Regulation 530-1, each 8A Staff Directorate maintains an OPSEC Officer for a total of 29 positions. 8A Major Subordinate Commands (MSCs), excluding war traced reserve units, account for an additional 82 primary and alternate OPSEC Officers.

b. The OPSEC Support Element (OSE) teaches a quarterly OPSEC Level II Course on the Korean Peninsula. We train roughly 30 personnel from 8A MSCs and Directorates per class. Each class comprises OPSEC primaries, alternates, and public affairs specialists. The 8A PM received OPSEC Level II training via the OSE OPSEC course in April 2015. The alternate 8A PM received Level II training via an Army OSE Mobile Training Team (MTT) in January 2015. In FY15, 8A conducted four OSE OPSEC Level II MTTs certifying 117 personnel (January: 35, April: 33, September: 22, and November: 27).

c. The 8A Commander's OPSEC policy and AK Regulation 530-1 are utilized by units. Soldiers receive OPSEC training within 30 days of arrival to their unit. Most units incorporate and track this as part of the unit in-processing checklist. OPSEC training for all 8A personnel, to include augmentees and participating Reserve and National Guard units, is mandated before every major exercise (Ulchi Freedom Guardian (UFG) and Key Resolve (KR)). MSCs also direct OPSEC refresher training prior to exercises conducted at their level such as the Second Infantry Division/Republic of Korea United States Combined Division's (2ID/RUCD) Warfighter Exercise held each fall. Additionally, 8A and several MSCs translate OPSEC training slides into Korean to ensure integration with host nation personnel.

EACS-D  
SUBJECT: Fiscal Year (FY) 2015 Annual OPSEC Report

3. Program plans and procedures.

a. OPSEC policies and planning guidance.

(1) AK Regulation 530-1, 09 January 2010 (currently under revision – anticipated publication date: January 2016).

(2) 8A Command Policy Letter #2 Operations Security (OPSEC) Policy, 23 November 2015.

(3) 8A OPORD 249-13 (8A OPSEC Program Base Order), 11 April 2013.

(4) FRAGO 1 to 8A OPORD 249-13, 18 July 2013.

(5) FRAGO 2 to 8A OPORD 249-13, 03 October 2013.

(6) FRAGO 3 to 8A OPORD 249-13, 26 November 2013.

(7) FRAGO 4 to 8A OPORD 249-13, 20 February 2014.

(8) 8A OPORD 14-09-12-01, 12 September 2014.

(9) FY16 Command Inspection Program (CIP) and Staff Inspection Program (SIP) Checklist Guide for OPSEC, 01 August 2015.

b. All OPSEC related plans and procedures may be found on the 8A web portal. This access-controlled portal ensures widest dissemination of the USARPAC, United States Forces Korea (USFK), and 8A Critical Information Lists (CIL), current OPSEC publications and references (Department of Defense (DoD) Instructions and Manuals, Army Regulations, USFK and 8A OPSEC Policy Letters, and Joint Publications), 8A CIP material, OPSEC training material, OPSEC posters, newsletters, and smart cards, and a range of template documents to enhance unit OPSEC programs. Additionally, it provides visibility on current and upcoming quarterly OSE OPSEC Level II certification courses and allows for online registration and course management. A separate access-controlled shared drive contains unit-specific plans, policies, and procedures, training certificates, security clearance verifications, and unit training rosters. Collectively, these two repositories serve as an OPSEC information clearinghouse and virtual record-keeping system. With the high transition rate in Korea, this online system ensures continuity is maintained across 8A OPSEC programs at the Theater Army, Division, and Separate Brigade and Battalion level.

EACS-D

SUBJECT: Fiscal Year (FY) 2015 Annual OPSEC Report

c. Per 8A OPORD 249-13 (8A OPSEC Program Base Order), "Directorates, MSCs, and supporting units will post their units CIL and, at a minimum, one additional OPSEC poster in a visible location in each primary office building." A check of this requirement is included within the CIP process. Some MSCs extended this requirement and have their CIL posted next to each workstation. 8A posts CIL, along with OPSEC awareness posters in all common areas during exercises to include barracks, Morale Welfare and Recreation (MWR) facilities, work areas and mayor cell locations. The two marquee bill boards on United States Army Garrison Yongsan (USAG-Y) are also used to post abbreviated CIL messages 45 days before and after each major exercise. MSCs tailor their OPSEC policy letter from the 8A policy letter.

d. Due to everyday real world potential conflict on the Korean Peninsula, CIL discussions remain flexible. The CIL is updated at the unit level with regard to change of mission or annually as needed. USFK and 8A publish exercise CILs before every major exercise and this is an additional product that is briefed to every member assigned, attached or serving in support of 8A. The recently revised 8A Policy Letter #2 (OPSEC) introduced a new CIL to reflect changes on the Korean Peninsula along with a leader's tool that crosswalks indicators and OPSEC measures to identified critical information.

e. 8A implements a 100% shred policy. MSCs utilize CIP inspections and Staff Assistance Visits (SAV) that stress the protection of Personal Identifiable Information (PII) and sensitive information for service members and their families. Badges for entrance into secure facilities, whether classified or sensitive in nature are utilized to limit personnel access to "need to know" only locations. Upon exiting the facility, a badge removal policy is enforced. All personnel assigned to 8A complete mandatory OPSEC training upon arrival to the unit, OPSEC refresher training is then conducted on a mandatory basis. As well, quarterly MTTs from OSE provide OPSEC Level II training to the command.

f. When conducting training, all members of the command are briefed on the importance of sharing sensitive information with only personnel that have an official need for the information, and not to give out information freely when asked.

g. MSCs perform dumpster inspections to ensure material is properly disposed. This helps in preventing unauthorized disclosures to adversaries. Units enforce shred policy and avoid placing data on SharePoint that compromises Soldiers privacy and upcoming operations activities. Secure voice and video systems are used to ensure meetings and discussions of a sensitive nature are secure.

EACS-D  
SUBJECT: Fiscal Year (FY) 2015 Annual OPSEC Report

h. 8A conducts media scans for information relating to 8A for potential OPSEC violations. All our open source material is given an OPSEC screening, and our MSCs have Public Affairs Office (PAO) personnel trained to conduct screenings, either External Official Presence (EOP) or OPSEC Level II training. The process used for release of information for public use is that all information being released for public consumption must go through the EOP or OPSEC Level II trained personnel.

i. The G2, G7, and PAO monitor open source release of information and links it to OPSEC considerations as appropriate. In addition, the G7 conducts a weekly Communication Strategy Working Group to implement all official messages and Commanding General guidance. These meetings also facilitate the OPSEC review process. Both the G7 and PAO maintain OPSEC level II Officers.

j. The G1 reviews all Freedom of Information Act (FOIA) requests utilizing the 8A CIL, five-step OPSEC process, and an 8A OPSEC specific checklist to screen all documentation prior to release. The checklist is maintained by the G1 and OPSEC PM for historical record keeping.

k. The 8A OPSEC PM reviews and screens all contracts for compliance.

l. Each 8A directorate has a minimum of one assigned Level II certified OPSEC officer responsible for reviewing, screening, and approving any publicly releasable documentation outside of PAO channels (e.g., professional journal articles, speeches, etc.).

#### 4. Assessments.

a. 8A OPSEC PM conducted nine SAVs and nine CIPs for MSCs. Additionally, all MSCs conducted CIPs of their subordinate commands. The SAV assessments were requested by MSCs to improve upon the shortcomings of their respective OPSEC programs.

b. USARPAC conducted an Organizational Inspection Program (OIP) inspection of 8A OPSEC in May 2015. USARPAC assessed 8A as having "exceeded USARPAC standards," and the USARPAC Deputy Commanding General – National Guard commended the 8A OPSEC program for its performance. Of the five (5) areas inspected, all exceeded USARPAC standards.

c. High personnel turnover in Korea challenges units' program continuity. 8A stresses continuity through SAVs and CIPs by reinforcing the need for thorough

EACS-D

SUBJECT: Fiscal Year (FY) 2015 Annual OPSEC Report

transitions and comprehensive historical record keeping. 8A portal enhancements greatly assist with increasing the level of continuity across the force.

d. Results of SAVs and CIPs indicate that CIL protection, familiarization and countermeasures are widely disseminated and practiced. Placards containing unit CIL, OPSEC measures and 100% shred reminders are prominently displayed in office work areas. Office work areas conspicuously label shred boxes and bags and clearly label non-shred containers. Personnel openly talk about and remind others about OPSEC enforcement and procedures. As previously mentioned, CIL and OPSEC awareness posters are prominently displayed in office work areas and common areas at exercise locations.

5. OPSEC training and awareness.

a. Soldiers and civilian personnel receive OPSEC training or refresher training within 30 days of their arrival or hiring and before major training events regardless of participation to ensure the force has a better understanding of OPSEC awareness and the dangers of unsecure information.

b. With the one to two year turn around on assignments in Korea, 8A training requirements are high. The 111 primary and alternate OPSEC Officer requirements and the one to two year Permanent Change of Station (PCS) cycle require multiple MTTs on the Korean peninsula. 8A requires a permanent General Schedule (GS) employee (Level III trained) in order to cut back on the travel requirements and costs associated with attending multiple MTTs per year.

c. The 8A OPSEC Program Manager participates in the quarterly 8A Protection Working Group, quarterly USAG-Y OPSEC Working Group, and a quarterly working group to address defense critical infrastructure.

6. Program Resources:

a. MTTs provide 8A the opportunity to school train their OPSEC PMs, Officers, and Coordinators at Brigade and Battalion level at no cost to the MSCs. Interagency OPSEC Support Staff (IOSS) awareness materials (posters and videos) posted in visible areas with high foot traffic and utilized during OPSEC refresher courses increased the abilities of the OPSEC PM to reach to the lowest levels. These materials are provided at no cost to the unit.

b. There were no funding shortfalls in FY15.

EACS-D  
SUBJECT: Fiscal Year (FY) 2015 Annual OPSEC Report

7. 8A continues to refine the training tools used to instruct the annual, refresher and exercise classes. 8A is focusing on training staff directorate OPSEC coordinators so they can assist with OPSEC awareness and review orders processes and contracts for OPSEC compliance within their own directorates.

8. 8A conducts quarterly OPSEC MTTs and published an order directing MSCs and staff directorates to have Soldiers trained. Approximately 30 personnel attend the training quarterly. 8A scheduled four OSE Level II MTTs in FY16 and anticipates training approximately 120 personnel next year. Additional emphasis will be placed on improving unit review processes, expanding Family Readiness Group (FRG) and webmaster OPSEC training, and incorporating measurable OPSEC objectives in major exercises.

9. Ninety four percent of 8A and subordinate MSCs are up to date with annual OPSEC awareness training. The shortage is due in part to personnel turn over. These individuals will be trained within 30 days of arrival to the unit and unit training records updated. Through CIPs, all MSCs demonstrated procedures to complete the training tasks. 8A and all MSCs do incorporate current, unclassified threat data corresponding with operations in the Korea.

10. Enclosure 1 discusses public facing websites throughout 8A MSCs.

11. Newly arrived Soldiers and Family members are provided instruction in protecting information, including information contained in social networking sites. FRGs are encouraged to stress the importance of information management and discuss what is acceptable to post on social networking sites.

12. Point of contact for this report is MAJ Matthew Woods, 8A OPSEC PM at DSN 315-723-3883 or [matthew.e.woods.mil@mail.mil](mailto:matthew.e.woods.mil@mail.mil). Alternate OPSEC PM is CPT Timothy Smith DSN 315-723-2704 or [timothy.l.smith19.mil@mail.mil](mailto:timothy.l.smith19.mil@mail.mil).

FOR THE COMMANDER:

1 Encl  
1. Unit Websites

  
SCOTT A. SHORE  
Colonel, GS  
Deputy Chief of Staff

Figure I-2. 8A Annual OPSEC Report Format

**Appendix J**

**Annual Army Operations Security Achievement Awards Program**

8A units seeking recognition for organizational or individual achievement should reference appendix J, AR 530-1 for awards criteria and submission requirements.

## **Appendix K**

### **8A Staff and Major Subordinate Commands**

#### **K-1. Staff Listing**

The following directorates are designated as 8A Staff for Organizational Inspection Program (OIP) and Command Inspection Program (CIP) purposes.

- a. SGS (Secretary of the General Staff)
- b. ACoS, G1 (Personnel)
- c. ACoS, G2 (Intelligence)
- d. ACoS, G3/5/7 (Operations and Maneuver)
- e. ACoS, G33 (Current Operations)
- f. ACoS, G34 (Protection)
- g. ACoS, G35 (Future Plans)
- h. ACoS, G37 (Training and Exercises)
- i. ACoS, G3 Aviation
- j. ACoS, G3 FSE
- k. ACoS, G4 (Sustainment)
- l. ACoS, G5 (Strategic Plans)
- m. ACoS, G6 (Command and Control)
- n. ACoS, G7 (Information Operations)
- o. ACoS, G9 (Civil Affairs Operations)
- p. ACoS, G3 Engineers
- q. PMO (Provost Marshal's Office)
- r. SJA (Staff Judge Advocate)
- s. IG (The Inspector General)
- t. Chaplain
- u. Surgeon
- v. 2501 Digital Liaison Detachment (DLD)
- w. 2502 Digital Liaison Detachment (DLD)

**K-2. Major Subordinate Command Listing**

The following elements are designated as 8A Major Subordinate Commands for Organizational Inspection Program (OIP) and Command Inspection Program (CIP) purposes.

- a. Second Infantry Division, R.O.K – U.S. Combined Division (2ID/RUCD)
- b. 19th Expeditionary Sustainment Command (19ESC)
- c. 501st Military Intelligence Brigade (501MI)
- d. 35th Air Defense Artillery Brigade (35ADA)
- e. 65th Medical Brigade (65MED)
- f. 1st Signal Brigade (1SIG)
- g. USFK Special Troops Battalion (USFK STB)
- h. Headquarters and Headquarters Battalion, Eighth Army (HHB 8A)
- i. 3rd Battlefield Coordination Detachment (3BCD)

## Appendix L

### Information That May Be Exempt from Release under the Freedom of Information Act

#### L-1. Exemptions

Only information that falls in the following categories may qualify as exempt from public disclosure under FOIA.

a. Exemption 1. Information which is currently and properly classified.

b. Exemption 2

(1) Information which pertains solely to the internal rules and practices of the agency. On March 7, 2011, the U.S. Supreme Court issued an opinion pertaining to Exemption 2 of FOIA (5 USC 552(b).2) that overturned 30 years of established FOIA precedents and significantly narrowed the scope of that exemption. See *Milner v. Dept of the Navy*, 131 S. Ct. 1259 (2011).

(2) Based on that text, and as set forth by the Supreme Court's decision in *Milner*, there are three elements that must be satisfied in order for information to fit within Exemption 2.

(a) The information must be related to "personnel" rules and practices.

(b) The information must relate "solely" to those personnel rules and practices.

(c) The information must be "internal."

(3) The language provided for exemption of matters "related solely to the internal personnel rules and practices of an agency" 5 (USC 552(b)(2)). Thus, the old formulations of "High 2" and "Low 2" - which were based on legislative history and not on this statutory language - no longer control. There is now just "Exemption 2" which is defined according to its text.

c. Exemption 3. Information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed.

d. Exemption 4. Information, such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis, which, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future, or protect the government's interest in compliance with program effectiveness.

e. Exemption 5. Intra-agency memoranda which are deliberative in nature; this exemption is appropriate for internal documents which are part of the decision making process and contains subjective evaluations, opinions, and recommendations.

f. Exemption 6. The release of information which could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.

g. Exemption 7. Records of information compiled for law enforcement purposes that:

(1) Could reasonably be expected to interfere with law enforcement proceedings.

(2) Would deprive a person of a right to a fair trial or impartial adjudication.

(3) Could reasonably be expected to constitute an unwarranted invasion of personal privacy of others.

(4) Disclose the identity of a confidential source.

(5) Disclose investigative techniques and procedures.

(6) Could reasonably be expected to endanger the life or physical safety of any individual.

*h.* Exemption 8. Certain records of agencies responsible for supervision of financial institutions.

*i.* Exemption 9. Geological and geophysical information concerning water and oil wells.

**L-2. References**

For more information on FOIA, refer to AR 25-55 and AR 380-5.

**Appendix M**

**Format for Operations Security Annex/Appendix/Tab to Operation Plan/Operation Order**

Units should refer to Figure M-1, Sample format for OPSEC annex/appendix/tab to OPORD/OPLAN, to AR 530-1 for further guidance.

## **Appendix N**

### **Format for Operations Security Documents**

Units should refer to Figures N-1, N-2, and N-3 to AR 530-1 for further guidance. These formats can serve as a guide when writing an OPSEC plan for activities, programs, or projects not documented by an OPORD or OPLAN.

## **Appendix O**

### **Internal Control Evaluation**

#### **O-1. Function**

The function covered by this evaluation is the implementation of Army OPSEC policy as outlined in this regulation.

#### **O-2. Purpose**

The purpose of this evaluation is to assist commanders at all levels in evaluating the following key internal controls contained in this regulation. It is not to cover all controls.

#### **O-3. Instructions**

These key controls must be formally evaluated at least once every 5 years or whenever internal controls administration changes. Certification that this evaluation has been conducted must be accomplished on DA Form 11-2 (Internal Control Evaluation Certification). Evaluation test questions are outlined in paragraph O-4, below and are intended as a start point for each applicable level of internal control. Answers must be based on actual testing of key internal controls. Answers that include deficiencies must be explained and the corrective action indicated in supporting documentation.

#### **O-4. Test Questions**

##### *a.* Establishment of OPSEC education and training.

(1) Has the DCS, G-3/5/7, through Commander, TRADOC, coordinated with Army training institutions to integrate OPSEC fully into curricula throughout officer, warrant officer, NCO and civilian education systems?

(2) Has the DCS, G-3/5/7, in coordination with Commander, 1st Information Operations Command (Land), completed an annual report describing the Army's progress in meeting DOD requirements for a trained OPSEC cadre with the DA Career Force.

(3) Has the Commander, 1st IO CMD(L) developed and is the 1st IO CMD(L) teaching the Army's HQDA PMs and OPSEC Officers course in sufficient iterations and quotas to train the force?

##### *b.* Implementation of responsibilities under this regulation.

(1) Has the DCS, G-3/5/7 developed OPSEC policies that are consistent with DOD and Joint policies, guidance and instructions?

(2) Have ACOMs, ASCCs, and DRUs appointed a non-contractor staff position to become the command's OPSEC PM?

(3) Is the Army OPSEC PM maintaining an archive of ACOMs, ASCCs, DRUs annual OPSEC reports that include Program Management, Program Plans and Procedures, assessments, and OPSEC Training and Awareness?

(4) Has the Army OPSEC PM established, chaired and managed an OPSEC Working Group comprised of ACOMs, ASCCs, and DRUs OPSEC PMs?

##### *c.* Development of OPSEC capability in the Army.

(1) Do personnel assigned to OPSEC PM/OPSEC Officer positions meet the eligibility criteria outlined in appendix H?

(2) Does the DCS, G-3/5/7, in coordination with the 1st IO CMD (L), maintain an OPSEC-trained personnel database to track OPSEC-trained personnel across the Army?

(3) Are Doctrine, Organization, Training, Material, Leadership and education, Personnel, Facilities solutions being applied to OPSEC shortfalls or problem sets identified by ACOMs, ASCCs, and DRUs?

**Appendix P**  
**OPSEC Assessment**

Units may use the All Purpose Checklist as a guide in performing OPSEC assessments of their organization.

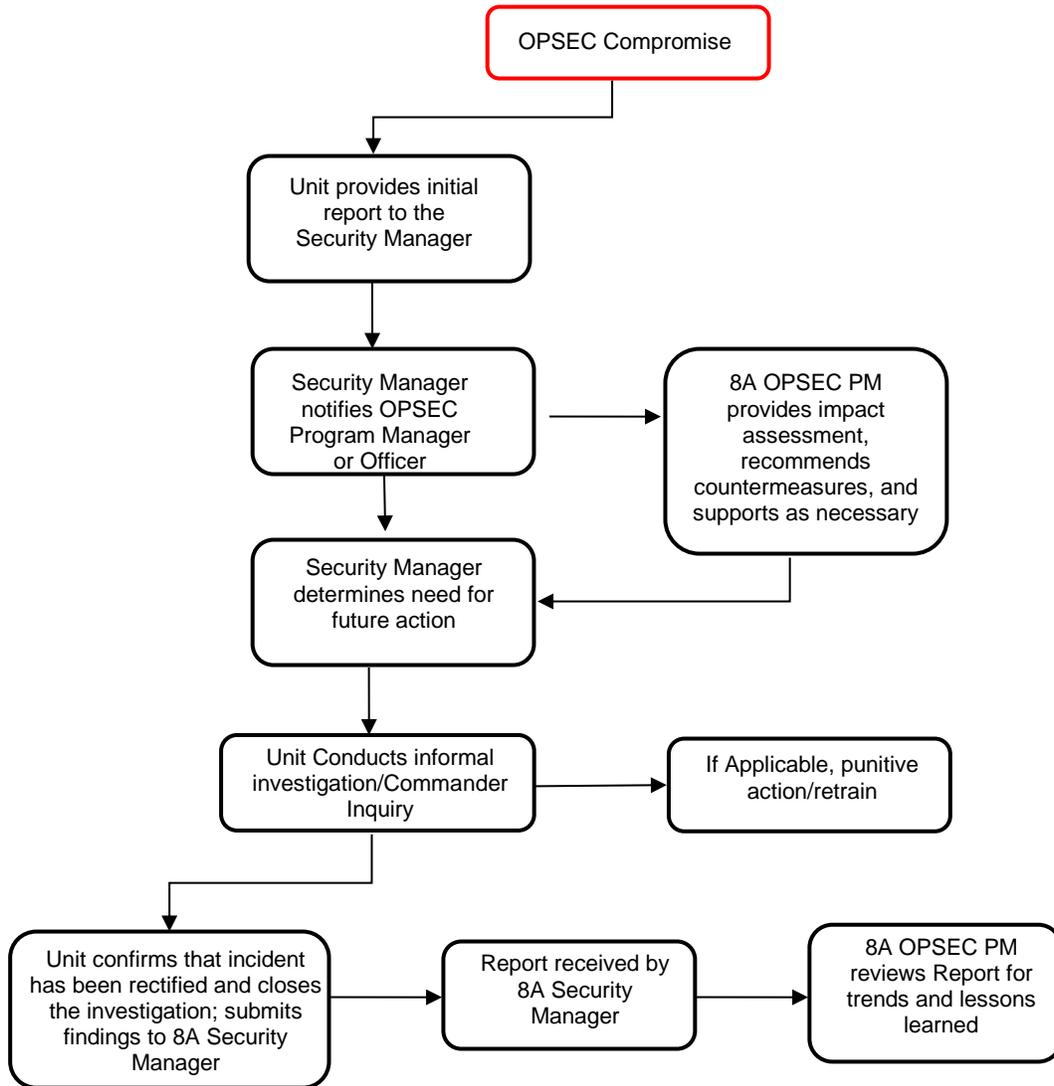
ALL PURPOSE CHECKLIST		PAGE 1 OF 2 PAGES		
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA		OPR	DATE	
Operations Security (OPSEC) Checklist				
N O.	ITEM ** Operations Security (OPSEC) ** <i>(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)</i>	YES	NO	N/A
	Program Reviewed:			
	Personnel Contacted:			
1.	Has the organization issued an OPSEC program implementing document?			
2.	Has an OPSEC program manager or OPSEC coordinator been appointed?			
3.	Are there specific requirements to include the OPSEC process in planning for and in the conduct of operations and other activities?			
4.	Is there a requirement to use OPSEC analytic techniques to assist in identifying vulnerabilities and to select appropriate OPSEC measures?			
5.	Have measures been taken to ensure that all personnel, commensurate with their positions and security clearances, are aware of adversary threat sources and understand the OPSEC process?			
6.	Are there periodic reviews and evaluations of organizational OPSEC activities by management? Are the results used in the improvement of OPSEC programs?			
7.	Where appropriate, does the OPSEC program extend to support and contractor organizations?			
8.	Is there an understanding that the OPSEC process is applied within an organization by using OPSEC planning or OPSEC surveys?			
9.	Is there an understanding by managers of what information is critical to the organization's mission effectiveness?			
10.	Is there an awareness that indicators derived from routine actions conducted in the normal conduct of operations or activities, even though unclassified, may provide adversaries with classified or sensitive critical information?			
11.	Is there an appreciation for the types of actions and activities that can be exploited through adversary collection and analysis?			
12.	Is there an understanding that all potential adversaries must be considered in developing the threat?			
13.	Is there an understanding that the organization's operations must be looked at from the adversary viewpoint and to do this tailored threat is required?			
14.	Is there an appreciation for the types of OPSEC measures that are available to remedy vulnerabilities (e.g., avoiding stereotyped procedures or activities; concealing unique activities or equipment; using deception to deal with indicators that can not be protected any other way; applying appropriate security measures to vulnerabilities; limiting and controlling distribution of unclassified documentation and data bases; reviewing and			

ALL PURPOSE CHECKLIST		PAGE 1	OF	
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA		2	PAGES	
Operations Security (OPSEC) Checklist		OPR	DATE	
	deleting indicators from documentation available for public release such as schedules, logistics, budgeting, travel, press releases, etc.)?			
15.	Is OPSEC, included in the organizations planning and program development processes for all organizational activities and operations beginning with initiation of the planning and program development process?			
16.	Is there an understanding of the types of adversary intelligence collection techniques that exist and of how to obtain tailored intelligence threat information to support the OPSEC program? Have requirements for appropriate tailored current intelligence threat information been submitted?			
17.	Have those areas, activities, functions, data or information about the organization's operations and activities deemed most important to keep from an adversary (i.e., critical information) been determined?			
18.	Have potential adversaries been identified (i.e., individuals, organizations or groups that must be denied critical information in order to maintain mission effectiveness)?			
19.	Are OPSEC initiatives, surveys, implementation of countermeasures and other OPSEC activities prioritized? Is the priority based on weighing the importance of the activity or operation, the sensitivity of the information involved, and the capabilities of the adversaries?			
20.	Are adequate records, plans and goals maintained to provide a basis for continuity in the organization's OPSEC program?			
21.	Does a mechanism exist for employees to raise OPSEC problems and provide suggestions to improve the organization's OPSEC program?			
22.	Have all problems encountered in establishing, and sustaining the organization's OPSEC program been reported to management?			
23.	Do personnel within the organization believe that management provides adequate support for the OPSEC program within the organization?			
24.	Do all individuals, commensurate with their position in the organization, understand the OPSEC process?			
25.	Are all individuals in the organization, commensurate with their position and security clearances, aware of the adversaries' capabilities to acquire critical information?			
26.	Are personnel in the organization aware of the formal OPSEC training available to the organization?			
27.	Have organizational OPSEC "lessons learned," highlighting both good and bad OPSEC practices, been incorporated into OPSEC awareness and training programs?			
28.	Does the organization employ a variety of methods, (i.e., posters, briefings, handbooks) as reminders, to maintain a high level of OPSEC awareness?			
29.	How is sensitive information handled by personnel?			
30.	Are there shredders available?			
31.	Check trash.			
32.	OPSEC Awareness Activities			

**Appendix Q**  
**OPSEC Compromise Procedures**

Units may use the following decision tree as a guide in reporting and investigating potential or real OPSEC compromises.

**8A OPSEC Reporting/Action Workflow**



OPSEC Compromise, AR 530-1, 1-5 b. (4) d.

1) An OPSEC compromise is the disclosure of sensitive and/or critical information that jeopardizes a unit's ability to execute its mission or to adequately protect its personnel and/or equipment or effects national security.

**Appendix R  
FOIA Cover Sheet**

The below cover sheet is an example. It may be employed by unit FOIA and/or OPSEC officers to document OPSEC reviews of FOIA requests.

<b>OPERATIONS SECURITY (OPSEC) REVIEW COVER SHEET</b> Freedom of Information Act (FOIA) Request	
FOIA Request Title: <u>&lt;Short Title&gt;</u>	Date: <u>&lt;DDMMYY&gt;</u>
Originating Authority: <u>&lt;Insert Requesting Organization&gt;</u>	
<b>Section I: Instructions</b>	
<p><u>Purpose:</u> The use of this cover sheet documents the unit's compliance with AR 530-1 in performing an OPSEC review of all FOIA requests received.</p> <p><u>Army Regulatory Requirement:</u> The OPSEC review is a documented evaluation of information or visual products intended for public release to ensure protection of critical and/or sensitive information. Products that may require an OPSEC review can include, but are not limited to, memorandum letters, e-mail messages, articles, speeches, academic papers, videos, briefings, contractual documents, news releases, technical documents, web content, proposals, plans, orders, response to FOIA and Privacy Act. When critical and/or sensitive information is found, corrective action will be recommended to the appropriate official in writing. Only information that falls in the nine categories outlined in AR 25-55, AR 380-5, or appendix L, AR 530-1 are exempt from public disclosure under FOIA. OPSEC coordinators, Web masters, PAOs, FOIA, speech writers, FRsAs, or any other personnel who interact with the public on a regular basis will receive external official presence (EOP) training or attend a Level II OPSEC officers course (AR 530-1).</p> <p><u>Mandatory Review and Signatures:</u> The organizational FOIA Officer or representative must review each FOIA request package prior to submission to the originating authority to include coordination with other staff elements for review as appropriate. The FOIA Officer and organizational OPSEC Program Manager/Coordinator/Officer will sign.</p>	
<b>Section II: Requirements</b>	<i>Check for Yes</i>
1. Determine if documentation meets any of the nine (9) FOIA exemptions	<input type="checkbox"/>
2. Screen for PPI/PII and Privacy Act information (consult G1)	<input type="checkbox"/>
3. Screen for HIPAA information (consult SURG)	<input type="checkbox"/>
4. Screen for financial data (consult COMP/FIN)	<input type="checkbox"/>
5. Screen for trade secrets, intellectual property, and Critical Program Information (CPI) (consult G8/Contracts)	<input type="checkbox"/>
6. Screen for Antiterrorism/Force Protection and Defense Critical Infrastructure Protection (DCIP) information (consult G34/OPD)	<input type="checkbox"/>
7. Screen for Law Enforcement Sensitive (LES) information (consult PMO)	<input type="checkbox"/>
8. Review for classification level, data aggregation, disclosure of sources, methods, and capabilities (consult G2)	<input type="checkbox"/>
9. Screen for Critical Information List (CIL) identified information and friendly detectable actions (Capabilities, Activities, Limitations, and Intentions) (consult G33 OPSEC)	<input type="checkbox"/>
10. Perform legal review (consult SJA)	<input type="checkbox"/>
11. Review redactions and advise necessary unit commander or chief advisor(s) (consult Chief of Staff or SGS)	<input type="checkbox"/>
<b>Section III: Remarks</b>	

<Insert Text>

**Section IV: Signature**

FOIA Officer: <Rank/Grade, First, Last>  
Typed or printed rank/grade and  
name

Signature:  
\_\_\_\_\_

Date: <DDMMYY>

Phone Number: <Insert DSN>

OPSEC Officer: <Rank/Grade, First, Last>  
Typed or printed rank/grade and  
name

Signature:  
\_\_\_\_\_

Date: <DDMMYY>

Phone Number: <Insert DSN>

**Appendix S**  
**Social Media Checklist**

The below checklist is an example. It may be employed to increase External Official Presence and general web safety.

<b>8A Social Media and Website Checklist</b>		
<b>Description</b>	<b>Yes/No</b>	<b>Remarks</b>
1	Does the Social Media/Web Site contain a clearly defined purpose statement that supports the mission of the DoD Component?	
2	Are users of this Social Media/Web Site provided with a privacy and security notice prominently displayed or announced on at least the first page of all major sections of each web information service?	
3	If applicable, does this Social Media/Web Site contain a Disclaimer for External Links notice, when a user requests any site outside of the official DoD web information service (usually a .mil or .gov domain)?	
4	Is this Social Media/Web Site free of commercial sponsorship and advertising?	
5	Does the Social Media/Web Site contain any information indicating plans or lessons learned which would reveal military operations, exercises or vulnerabilities?	
6	Does the Social Media/Web Site reference any information that would reveal sensitive movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of the security of a military plan or program?	
7	Does the Social Media/Web Site contain movement of key personnel (schedules, security details, addresses, etc.)?	
8	Does the Social Media/Web Site contain transportation plans?	
9	Does the Social Media/Web Site contain unit vulnerabilities and weaknesses?	
10	Does the Social Media/Web Site contain personnel documents and rosters?	
11	Does the Social Media/Web Site contain social security numbers?	
12	Does the Social Media/Web Site contain dates of birth?	
13	Does the Social Media/Web Site contain home addresses?	
14	Does the Social Media/Web Site contain personal phone numbers?	
15	Does the Social Media/Web Site contain names and locations of family members?	
16	Does the Social Media/Web Site follow unit public affairs guidance?	

## **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
CAO	Civil Affairs 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
ELINT	Electronic Intelligence
ELSEC	Electronic Security
EMCON	Emission Control
EOP	External Official Presence

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
MSC	Major Subordinate Command
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
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
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**

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.

**Critical Information List (CIL)**

Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively, so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.

**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.

**Defense Critical Infrastructure**

The composite of DoD and non-DoD assets essential to project, support, and sustain military forces and operations worldwide.

**Defense Critical Infrastructure Program**

A DoD risk management program that seeks to ensure the availability of Defense Critical Infrastructure.

**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 Secrecy**

The condition achieved from 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.

**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 uses; 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)**

(DOD) The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. Also called IO.

**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.

**Military Information Support 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 military information support operations is to induce or reinforce foreign attitudes and behavior favorable 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; 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
- b. 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.

### **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.

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.