

CESWL-SL

DEPARTMENT OF THE ARMY  
LITTLE ROCK DISTRICT, CORPS OF ENGINEERS  
LITTLE ROCK, ARKANSAS 72203-0867

SWLR 530-1-1

Regulation  
No. 530-1-1

3 May 1999

Military Operations  
OPERATIONS SECURITY (OPSEC)  
STANDARD OPERATING PROCEDURE (SOP)

1. Purpose. To provide policy and guidance for operations security (OPSEC) within Little Rock District, U.S. Army Corps of Engineers, Little Rock, Arkansas.

2. References.

- a. AR 380-5, Department of the Army Information Security Program.
- b. AR 525-13, U.S. Army Combating Terrorism Program
- c. AR 530-1, Operations Security (OPSEC).
- d. Joint Pub 3-54, Joint Doctrine for Operations Security.
- e. JCS Pub Joint Operation Planning Execution System, Vol I & II.
- f. CJCS MOP 30, Command and Control Warfare (C2W).
- g. CJCS Instruction 3213.01, Joint Operations Security
- h. FM 100-6, Information Operations

3. General.

a. The objective of OPSEC is to preserve the effectiveness of military capabilities; and maintain the elements of initiative, surprise, and security. The purpose of this Standard Operating Procedure is to provide Little Rock District personnel guidance for the implementation of OPSEC within the District.

b. To be effective, Operations Security must begin early in planning when a commander identifies a need to gain and maintain essential secrecy. Essential secrecy depends on traditional

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

SWLR 530-1-1

3 May 99

security programs to deny classified information; and OPSEC measures to identify, control and protect indicators that may in an aggregate form disclose classified or sensitive information. OPSEC measures occur during the planning, preparation, execution and post-execution of operations and activities.

c. Adversaries depend on detectable activities and open sources for information about project and mission intentions and capabilities. Operations (training, tests, exercises, development, deployments etc.) involve many detectable (observable) activities and significant amounts of open source information. As world conditions change, today's ally may be tomorrow's adversary or competitor.

4. Definition.

a. Operations Security (OPSEC). A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and activities to:

(1) Identify actions that can be observed (by any means) by adversaries intelligence systems.

(2) Determine indicators that could be interpreted or pieced together to derive critical information about our capabilities, intentions and activities.

(3) Select and execute measures that eliminate or reduce to an acceptable level friendly vulnerabilities to adversary actions.

5. Responsibilities.

a. Commander.

(1) Ensure OPSEC measures are implemented within the Little Rock District to preserve essential secrecy.

(2) Integrate OPSEC into all activities to provide maximum protection of all functions and activities.

(3) Implement these OPSEC Standard Operating Procedures.

FOR OFFICIAL USE ONLY

SWLR 530-1-1  
3 May 99

(4) Appoint/designate in writing an OPSEC Officer.

(5) Ensure OPSEC training is conducted IAW Annex F.

b. OPSEC Officer.

(1) Prepare and recommend OPSEC measures for all elements of the Little Rock District.

(2) Provide OPSEC guidance during the preparation of plans and other mission documentation, to include Force Protection.

(3) Develop and recommend Essential Elements of Friendly Information (EEFI).

(4) Conduct OPSEC reviews of documents.

(5) Ensure that OPSEC training is conducted IAW AR 530-1, and Annex F, of this SOP.

(6) Perform other duties and responsibilities as required.

(7) Coordinate with unit Force Protection/Combating Terrorism officer, Public Affairs and Freedom of Information Act officers' to ensure an OPSEC review is conducted prior to the release of information concerning the command, or command programs, projects, activities or operations.

(8) Conduct OPSEC awareness briefings for newly assigned personnel and employees on an annual basis, and as required for foreign travel.

c. All personnel assigned or attached to the Little Rock District.

(1) Comply with established OPSEC and security practices for the protection and control of critical information.

(2) Know Essential Elements of Friendly Information (EEFI) (Annex A)

FOR OFFICIAL USE ONLY

SWLR 530-1-1  
3 May 99

(3) Be aware of the adversary intelligence collection threat.

(4) Be familiar with contents of this SOP and where to obtain additional OPSEC guidance if needed.

6. Collection Threat. Adversaries using various intelligence collection methods may conduct collection of information on US Army activities. Many of these pieces of information are unclassified, but provide an accurate portrayal of the Districts mission and the commands overall intentions and or operations.

a. Human Intelligence Threat (HUMINT). HUMINT is the collection of information by human sources for intelligence purposes. Gathered covertly by espionage agents, or overtly through information available to the general public, open sources, which is the most basic form of intelligence collection. HUMINT remains significant because it is often the only source with access to an opponent's intentions and plans.

b. Imagery Intelligence Threat (IMINT). IMINT is the collection of information by photographic, infrared or radar imagery. Images can be gathered either by individuals or by remote means, such as aircraft or satellite. This method is valuable because it provides analysts with indicators of areas requiring examination by other means. Any form of imagery is IMINT.

c. Signals Intelligence (SIGINT). SIGINT is the collection of information by interception of electronic signals from communications equipment or non-communicative devices that emit an electronic signal, such as radar beacon. It includes interception of communications as well as the intercept and analysis of communication between pieces of equipment (e.g. computer networks).

d. Measurement and Signature Intelligence (MASINT). MASINT is scientific and technical intelligence obtained by quantitative and qualitative analysis of data derived from technical sensors to identify any distinctive features associated with the source, emitter or sender. (E.g. Acoustic, Radiation, Seismic etc.) It is highly technical in nature, and can be initiated remotely.

7. OPSEC Process. The OPSEC process applies to all phases of an activity, function or operation and is used in the development of OPSEC plans. The five fundamental steps are:

a. Identification of Critical Information. Critical information is needed by adversaries to effectively plan and act to degrade the operational effectiveness of the command. The development of Essential Elements of Friendly Information (EEFI) is part of the OPSEC process. EEFI are the key questions about friendly intentions, capabilities and activities, ask by adversary decision-makers. The EEFI list may be classified. Remember, that EEFI are the questions the adversary is going to ask, the answers to the questions are the items that must be protected. When traditional security programs cannot maintain protection, OPSEC must provide an OPSEC measure. (See Annex E, OPSEC Terms)

b. Analysis of Threat. Adversary collection efforts are identified. The aim is to neutralize or manipulate the threat to the US's advantage. The five questions that must be answered are:

(1) What critical information is already known by the adversary?

(2) What gaps exist in the adversary information base that prevent him from deriving critical information?

(3) What intelligence collection assets are available to the adversary that will enable exploitation of observed friendly indicators?

(4) What friendly actions might reveal critical information? (OPSEC Indicators, See ANNEX B, Sample OPSEC Indicators and E, OPSEC Terms)

(5) What are the potential OPSEC vulnerabilities?

c. Analysis of Vulnerabilities. Analysis of vulnerabilities identifies tentative OPSEC measures required to maintain essential secrecy. The most desirable OPSEC measure combines the highest protection with the least effect on mission operational effectiveness. There are three categories of OPSEC measures. (See Annex C, Sample OPSEC Vulnerabilities and E, OPSEC Terms)

FOR OFFICIAL USE ONLY

SWLR 530-1-1

3 May 99

(1) Action control -- Alternative ways of conducting actions and activities which avoid indicators which create vulnerabilities. Actions taken by/within District to eliminate (prevent) or control indicators.

(2) Countermeasures -- Disruption of adversary information collection or gathering.

(3) Counter Analysis -- Actions to cause misinterpretation of indicators by analysts.

d. Assessment of Risk. Because implementation of OPSEC measures usually presents a risk to operational, logistic or procedural effectiveness, an analysis must be made prior to the decision to implement measure. The OPSEC Officer makes recommendations on each measure based on these questions:

(1) What is the risk to mission/operation effectiveness if an OPSEC measure is implemented?

(2) What is the risk to the operation and the command mission success if an OPSEC measure is not implemented?

(3) What risk is likely to result if the OPSEC measures fail to be effective? Only the Commander can approve each OPSEC measure based on the answers to these questions. After these questions are answered, two decisions must be made.

(a) Which, if any, OPSEC, measures should be implemented?

(b) When should selected OPSEC measures be implemented?

e. Application of Appropriate OPSEC measures. OPSEC measures are selected based on decisions in the previous steps.

8. OPSEC Measures. Specific OPSEC measures must be developed for separate activities or operations. Assistance in the development of OPSEC measures is available from the District OPSEC Officer. The measures listed here are offered as a guide and as measures that are required for all activities. Personnel

FOR OFFICIAL USE ONLY

SWLR 530-1-1  
3 May 99

within the District are to use these measures in all activities:

a. Administrative Measures.

(1) Avoid open posting of planning schedule notices that reveal when sensitive events will occur.

(2) Control the issuance of orders, movement of personnel, programs etc., or key personnel.

(3) Control trash and housekeeping functions to conceal sensitive activities.

(4) During periods of increased mission/operational activity, follow normal leave policy and working hours to maximum extent possible to preserve the outward sense of normalcy.

(5) Ensure personnel maintain the ability, as necessary, to travel so that preparation for sensitive travel will not generate unusual activity.

(6) Screen discussions or releases to the media with public affairs personnel.

(7) Control access to sensitive/restricted areas and escort those personnel not assigned (Contracting Division, Cost Engineering).

(8) Be prepared to implement a "Clean Desk" on 1-hour notice in the event of visitors arrival.

b. Communications Measures.

(1) Make maximum use of secure communications. Telephone and FAX.

(2) Limit release of information until latest possible date or until activities are complete.

(3) Limit reading file distribution to personnel with need to know. Control distribution of controlled unclassified information (CUI) information IAW the distribution markings for

FOR OFFICIAL USE ONLY

SWLR 530-1-1

3 May 99

technical and operational information as stated in DoD Directive 5230.24 and the requirements stated in the EEFI list.

(4) Strict compliance with command AIS/ISS policy on the use of all computer system operation to include small computers.

c. Readiness Measures.

(1) Safeguard reports on unit personnel to include attendance at special schools.

(2) Limit distribution on rosters that identify personnel by position, MOS/Series, grade, or security clearance.

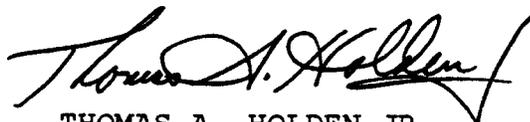
d. Travel Measures.

(1) Military personnel should travel in civilian clothes whenever possible. Do not carry briefcase, or bags that identify you as a member or employee of the command.

(2) Use a passport in lieu of military orders whenever possible.

(3) Do not discuss assignment, duties or reason for travel unless absolutely necessary (e.g. with security, customs or immigration personnel).

(4) Attend a Foreign Travel advisory briefing prior to any foreign travel IAW the Force Protection program.



THOMAS A. HOLDEN JR  
Colonel, Corps of Engineers  
Commanding

5 Encls

ANNEX A - ESSENTIAL ELEMENTS OF INFORMATION (EEFI)

ANNEX B - SAMPLE INDICATORS

ANNEX C - SAMPLE VULNERABILITIES

ANNEX E - OPSEC TRAINING

ANNEX F - OPSEC TERMS

FOR OFFICIAL USE ONLY

SWLR 530-1-1  
3 May 99

FOR OFFICIAL USE ONLY

**FOR OFFICIAL USE ONLY**  
**ANNEX A, ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION, TO LITTLE  
ROCK DISTRICT OPSEC SOP**

Essential Elements of Friendly Information are key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities so they can obtain answers critical to their operational effectiveness. Answers to the EEFI constitute critical information that must be protected. The EEFI below are common to all many types of activities and form the basis for specific EEFI for each activity and operation.

1. What missions and contingencies are being planned?
2. What AIS systems are in use?
3. What contracts contain classified or sensitive elements?
4. Where are the command and control nodes? Support activities?
5. What are current and planned command and control arrangements?
6. Which computers are capable of processing classified/sensitive information? Which ones are connected to a LAN?
7. What are the security procedures within the AIS?
8. Is there a secure telephone directory in use? Is it controlled?
9. Where are key personnel going TDY? What are the purposes of their TDY?
10. What are the methods used to carry information while on TDY?
11. What nations have exchange officers here, for what training?
12. Are there unannounced security inspections, such as trash containers?
13. What are the intended counter (terrorist, narcotics, etc.) operations, procedures?

**FOR OFFICIAL USE ONLY**

SWLR 530-1-1  
3 May 99

14. What counterintelligence support activities are ongoing?
15. Are there deceptions planned? In operation? Who is conducting?
16. What political constraints have been placed on planning, activities or operations?
17. What are the emergency action procedures? Who is contacted?

3 May 99

FOR OFFICIAL USE ONLY

ANNEX B, SAMPLE OPSEC INDICATORS, TO LITTLE ROCK DISTRICT OPSEC SOP

1. Indicators. Indicators are friendly detectable actions and open source information that can be interpreted or pieced together by an adversary to derive critical information. They are categorized as--

a. Profile Indicators - Information about a unit or activity which shows normal operation, functional capability, and routine procedures.

b. Deviation Indicators - Information which shows changes to standard or normal operations or activities.

c. Tip-off Indicators - Information which points to an operation, activity, event, capability or intention, and needs no other explanation.

*This listing is provided to give managers an idea of some of the actions or information which can provide indication of what has happened, is happening, or is going to happen. It is not all inclusive. These indicators must be looked at from the adversary point of view. Think of the indicators as being pieces of a large puzzle, as he collects each piece, the picture comes together. The adversary may not need every piece of the puzzle to see the overall picture of what we are doing. Specific indicators will be based on the actual activity.*

2. Administration.

- a. TDY Orders.
- b. Meeting or conference notification.
- c. Transportation, housing arrangements.
- d. Individual or District schedules.
- e. Changes to administrative workload.
- f. Changes to distribution plans.
- g. Use of words indicating irregular activity (e.g. Critical, Priority, Rush, Sensitive).
- h. Changes to personnel assignments.
- i. Security Classification Guides.
- j. Unusual security clearance requirements.
- k. Tables of Organization and Equipment/distribution and Allowances (TOE/TDA).
- l. Unit readiness reports, or information which is a component of the report (e.g. personnel assigned).

3 May 99

**FOR OFFICIAL USE ONLY**

- m. Canceling leaves/recalling personnel to unit.
- n. Changes to restricted areas or controlled access areas.

**3. Activities.**

- a. Changes in THREATCON.
- b. Repositioning of command assets.
- c. Deviations/cancellation of training.
- d. Increased activities by special units.
- e. Change in normal training activities including language training and special training.
- f. Conduct of security briefings.
- g. Movement of specially qualified personnel.
- h. Friendly reactions to national level exercises or hostile actions.
- i. Information on unit SOPs.
- j. Assignment of Liaison Officers.
- k. Conduct of rehearsals/exercises.
- l. Unprogrammed changes to in place security measures.
- m. Increase in contracting activity.

**4. Communications.**

- a. Increased volume of message traffic/secure communications.
- b. Changes to normal reporting procedures.
- c. Changes to reporting procedures/schedules.
- d. Imposition of COMSEC procedures.
- e. Increased coordination among headquarters.

**5. Intelligence.**

- a. Increased requests for area/country studies.
- b. Special requests for maps.
- c. Priority requests for threat briefings.

**6. Supply and Logistical Support.**

- a. Increased volume and priority of requisitions.
- b. Pre-positioning or movement of equipment.
- c. Requests for special equipment/munitions.
- d. Increased maintenance activities.
- e. Transportation requests.
- f. Requests for medical/transportation support.
- g. Increased or unusual requests for computer support

3 May 99

FOR OFFICIAL USE ONLY

ANNEX C, SAMPLE OPSEC VULNERABILITIES, TO LITTLE ROCK DISTRICT  
OPSEC SOP

1. Vulnerabilities. Vulnerabilities are friendly actions, which provide indicators that may be obtained and accurately evaluated by an adversary to provide a basis for effective adversary decision making. Vulnerabilities consist of stereotyped actions that habitually occur (patterns), and unique, detectable characteristics that identify a type activity or intention (signatures). These actions are the target of adversary intelligence collection efforts and should be considered when developing OPSEC measures. An OPSEC vulnerability exists when these conditions are exist:

a. An indicator is observable and adversary has the capability to collect the indicator.

b. The adversary has the time to collect, report, analyze, make a decision and react or take an action which will be harmful to our activities or mission.

2. Examples of Vulnerabilities:

a. Failure to ensure that sensitive information is furnished to authorized persons only.

b. Inadvertent disclosure of classified, and unclassified sensitive information.

c. Failure to follow security classification guidelines.

d. Unescorted visitors in areas with open storage of classified or sensitive information, or unclassified sensitive information, or exposure of indicators.

e. Improper storage or handling of classified documents.

f. Publication and distribution of information without distribution statements or an OPSEC and PAO review.

h. Failure to properly clear computer or automated information systems prior to allowing uncleared personnel to perform maintenance.

3 May 99

- i. Allowing maintenance personnel to work on information systems unsupervised.
- j. Assignment of uncleared personnel to duties that provide opportunity for access to unclassified sensitive information.
- k. Inadvertent release of information to the media.
- l. Improper disposal of unclassified sensitive or classified information.
- m. Carelessness in OPSEC implementing procedures.
- n. Failure to periodically review for compliance security and OPSEC procedures and requirements.
- o. Failure to maintain or enforce physical and automated access controls.
- p. Failure to brief newly assigned personnel on internal OPSEC procedures and measures.
- q. Failure to ensure all personnel are briefed and updated to the current collection threat, and FIS operations and activities.

ANNEX D, OPSEC TRAINING, TO LITTLE ROCK DISTRICT OPSEC SOP

1. Reference. AR 530-1
2. Operations Security Training. Within the Little Rock District OPSEC training is mandatory IAW reference 1. Three types of OPSEC training are required:
  - a. New arrival training (within 90 day of assignment to District)
  - b. OPSEC Officer advanced training (for personnel appointed as OPSEC Officers)
  - c. OPSEC awareness training (periodic throughout the year, prior to all deployments, and upon receipt of a THREATCON CHANGE FROM NORMAL)

OPSEC TERMS:

a. Adversary. Those individuals, groups or organizations that must be denied critical information to maintain friendly mission effectiveness. Adversaries may include hostile countries, terrorists, the media and allied intelligence agencies.

b. Critical Information. Specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and act to guarantee the failure of friendly mission accomplishment.

c. Essential Elements of Information (EEFI). Key questions adversaries are likely to ask about friendly intentions, capabilities, and actions so they can obtain answers critical to their operational effectiveness. District EEFI is at Annex A.

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

e. Indicators. Friendly detectable actions and open source information that can be interpreted or pierced together by an adversary to derive critical information. A list of possible indicators are at Annex B.

f. Sensitive Information. Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal program, but which has not been specifically authorized under an Executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy (PL100-235, 8 Jan 88)

g. Vulnerabilities. Friendly actions which provide indicators and may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary Decision-making. Vulnerabilities exist when three conditions coincide or exist -- Adversary has capability to collect indicator, and adversary has time to process (report, analyze, take planning action) and the adversary must be able to react. A list of vulnerabilities is at Annex C.

3 May 99

**FOR OFFICIAL USE ONLY**

h. Deception. Deception is an effective OPSEC measure, which can be employed given prior coordination. It can be used for the following reasons.

(1) Cause adversaries intelligence collection efforts to fail to target friendly activities.

(2) Create confusion or misinterpretation of information by an adversary analyst.

(3) Cause loss of interest by adversary observers.

(4) To withhold or confuse actual critical information.