

HEADQUARTERS  
UNITED STATES EUROPEAN COMMAND  
UNIT 30400  
APO AE 09131

DIRECTIVE  
NUMBER 55-9

8 March 2001

**OPERATIONS**

Operations Security

---

1. **Summary.** This directive stresses the importance of OPSEC in planning and executing EUCOM operations, and establishes OPSEC policy, procedures and guidance in the theater.
2. **Applicability.** Applies to the United States European Command and all of its components.
3. **Internal Control Systems.** This Directive contains internal control provisions and is subject to the requirements of the internal management control program. For HQ USEUCOM and subordinate joint activities, the applicable internal control directive is ED 50-8, Internal Management Control Program.
4. **Suggested Improvements.** Users can send suggestions for improving this directive to Headquarters, United States European Command, Operations Directorate, Information Operations Division (ECJ39), Unit 30400 Box 1000, APO AE 09128.
5. **References.**
  - a. Chairman of the Joint Staff (CJSC) Instruction 3213.01 "Joint Operations Security", dated 1 December 1997
  - b. Joint Pub 3-13 for Information Operations, dated 9 October 1998
  - c. Joint Pub 3-54 for Operations Security, dated 24 January 1997
  - d. DOD Directive 5200.7, Inspector Generals of the Unified and Specified Combatant Commands, 7 Jan 93, with Change 1, 21 May 93
6. **Explanation of Terms.** See Appendix A.
7. **Background.**
  - a. Joint Pub 3-54, reference (a), defines OPSEC as the process of identifying critical information and of subsequently analyzing friendly actions attendant to military operations and other activities to:

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

b. The Necessity for OPSEC.

(1). EUCOM's mission and the locations of our forces in foreign nations demand we develop and rigidly adhere to OPSEC procedures that protect our critical information. Our adversaries are looking for our OPSEC failures so they can use them against us to jeopardize our operations, facilities, and our personnel. Our adversaries are actively engaged in collecting intelligence against us to obtain diplomatic, economic and military advantage. Much of this information is gained through open source material (including media and the Internet) and observations of EUCOM activities and operations. This use of open sources is particularly true of terrorist groups.

(2). The goal of OPSEC is to control information and observable actions about friendly force capabilities, limitations and intentions so as to prevent or control their exploitation by an adversary. To achieve this goal, everyone in EUCOM must work together to identify what information and observable actions are critical to protect our operations, and take appropriate measures to ensure their security is maintained. OPSEC measures are essential for success, and apply during: all EUCOM operations whether in war, crisis or peace; during development of plans and orders; and during force protection planning.

c. OPSEC and IO, IW and C2W. OPSEC is an operational function. OPSEC, along with military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction are the elements of Information Operations (IO). IO are actions taken to affect an adversary's information and information systems while defending one's own information and information systems. OPSEC is an essential aspect of Information Warfare (IW), IO conducted in crisis, for ensuring the essential secrecy necessary for success. During Command and Control Warfare (C2W) OPSEC should be fully integrated with the other elements of IO, and fully supported by intelligence to deny, degrade, disrupt or destroy adversary command and control capabilities.

d. OPSEC and, Security and Counterintelligence. OPSEC is not a security function, though it requires close integration with various traditional security programs. OPSEC and security programs are mutually supportive, and must rely upon each other to provide essential secrecy. Counterintelligence supports both OPSEC and security programs. OPSEC does not replace the traditional security programs (physical security, personnel security, computer security, and information security), which are oriented toward protecting classified information. Similarly, OPSEC does not replace counterintelligence, which seeks to protect the command from espionage, other intelligence activities,

sabotage, or assassinations conducted by hostile elements. OPSEC complements those programs by denying our adversaries publicly available indicators of sensitive or classified activities, capabilities or intentions.

e. OPSEC and Operational Effectiveness. The ultimate goal of OPSEC is to increase operational effectiveness. This involves preventing the enemy from determining what, where, when, and how friendly operations will occur, until it is too late for enemy forces to effectively react to those operations. However, the commander must constantly balance the information that must be denied to adversaries against what must be known by friendly forces. Inadequate protection degrades operational effectiveness by hindering the achievement of surprise, while excessive protection may impede effectiveness by interfering with coordination, training or support. Proper use of the OPSEC process, as identified in reference c, will minimize the conflict between operational and security requirements.

8. OPSEC Program. Commanders are required to establish and maintain formal OPSEC programs. The OPSEC program supports the commander by ensuring the command practices OPSEC to deny critical information to adversaries. A viable OPSEC programs provides planning, training, education and evaluation.

a. Command Involvement. OPSEC is a command responsibility. As such, OPSEC planning guidance will be developed early and applied at all command levels for military operations, exercises, and activities which, if unprotected, could reveal sensitive operational capabilities, weapon system capabilities, plans, and/or procedures. Commanders will maintain and periodically review their Critical Information Lists (CIL).

b. Operational Orientation. OPSEC is an operational function, and requires full integration in all operational planning and execution. Therefore, responsibility for OPSEC should reside within the operations staff.

c. Integration. All staff elements must be involved in the development of CIL and Essential Elements of Friendly Information (EEFI), and must adhere to OPSEC procedures directed by the commander.

d. Training and Education. OPSEC training programs will be established to develop and maintain an optimal level of OPSEC knowledge among all members of assigned military forces and the DOD civilian work force. OPSEC officers will receive training to ensure they can implement the OPSEC program.

e. Annual Reviews and Surveys. All commanders need to conduct OPSEC surveys and annual reviews to determine the effectiveness of their OSPEC programs. These snap shots allow commanders to identify requirements for additional measures and make necessary changes in existing measures.

9. OPSEC Process. Commanders and their OPSEC planners will apply the OPSEC process to campaigns, deliberate and crisis action planning, and execution of operations. OPSEC's most important

aspect is that it is a process rather than collection of specific rules and instructions that can be applied to every operation. This process will help ensure the commander's OPSEC procedures appropriately counter the threat while meeting operations imperatives. This process is continuous and iterative. The full process is described in reference c. The five elements of the process are:

- a. Identification of critical information.
- b. Analysis of threats.
- c. Analysis of vulnerabilities.
- d. Assessment of risks.
- e. Application of appropriate OPSEC measures.

#### 10. Responsibilities.

##### a. HQ USEUCOM.

###### (1) The Chief of Staff will:

- (a) Provide command guidance for achieving JCS and EUCOM OPSEC objectives.
- (b) Approve the Critical Information Lists for HQ USEUCOM.
- (c) Develop OPSEC policy applicable to USEUCOM.
- (d) Approve the conduct of and review OPSEC surveys/operations security evaluations (OSE). (Ref Appendix C)
- (e) Provide command review and direction to the EUCOM OPSEC program.

###### (2) The Director of Operations, ECJ3 will:

- (a) Act as the office of primary responsibility for the HQ USEUCOM OPSEC program.
- (b) Direct accomplishment of OPSEC surveys/OSEs and preparation of reports, as appropriate.
- (c) Maintain liaison with other agencies, activities, and commands for the purpose of exchanging OPSEC items of interest.

(d) In accordance with CJCSI 3213.01A, Joint Operations Security submits annual OPSEC program reports, as of 31 July to arrive at the office of the Joint Chiefs of Staff by 1 September, in accordance with reference a.

(e) Serve as the U.S. representative to SHAPE on all in theater OPSEC matters as directed by JCS.

(f) Develop, review, or approve OPSEC annexes for USCINCEUR plans, as appropriate.

(g) Approve annual EUCOM request to NSA for Joint COMSEC Monitoring Activity (JCMA) support of EUCOM operations and exercises.

(h) Coordinate with the EUCOM J6 NSA LNO to determine appropriate actions if JCMA reports or other official reports indicate there has been a compromise of critical information.

(3) The Information Operations Division Chief, ECJ39 will:

(a) Develop and maintain the HQ USEUCOM OPSEC Program to include writing the organization's policy and guidance documents.

(b) Chair the EUCOM OPSEC Core Group (EOCG) consisting of representatives from the, Intelligence, Counter-Intelligence, Security Matters, Inspector General, Plans and Policy, Command, Control, and Communications Systems, and Public Affairs Directorates. Produce minutes of the OPSEC EOCG and distribute them to all HQ USEUCOM OPSEC officers. The EOCG will oversee OPSEC matters on a continuing basis. It will meet quarterly, or as directed by the chairman, to:

- o Identify and pursue headquarters initiatives on EUCOM OPSEC.
- o Provide stimulation to the HQ USEUCOM OPSEC program.
- o Coordinate internal OPSEC surveys and evaluations.

(c) Train HQ USEUCOM OPSEC Officers and assist them in developing directorate OPSEC programs.

(d) Maintain and update the list of all HQ USEUCOM OPSEC officers.

(e) Develop and review OPSEC annexes for USCINCEUR plans, as appropriate.

(f) Serve as liaison between Component OPSEC Officers to enhance EUCOM OPSEC.

(4) The Director of Intelligence, ECJ2 will:

(a) Disseminate hostile intelligence collection threat information and intelligence to the staff, appropriate commands, and ODCs.

(b) Provide assessments of hostile intelligence collection threats in support of EUCOM planning, operations, and OPSEC measures development. .

(c) Provide advice and assistance on the development and evaluation of OPSEC measures to counter the hostile intelligence collection threat.

(5) The Director of Command, Control, and Communications Systems, ECJ6 will:

(a) Manage Information Assurance (IA) programs and operations in USEUCOM and exercises staff supervision over COMSEC monitoring and analysis activities initiated in support of USEUCOM OPSEC program.

(b) Provide advice and assistance regarding National and Theater IA directives and their application to OPSEC.

(c) Provide briefings on COMSEC capabilities and limitations, as required.

(d) Evaluate IA support of joint operations and exercises to determine the effectiveness of COMSEC planning and actions which can/should be taken to correct COMSEC weaknesses and, therefore, improve force OPSEC posture.

(e) Initiate and promulgate instructions for IA improvement in support of OPSEC goals/objectives.

(f) Act as Executive Agent for management of designated USEUCOM/COMSEC surveillance missions.

(g) Determine and coordinate USEUCOM joint and combined communications security equipment and material requirements, including joint and combined tactical force requirements, in support of OPSEC surveys.

(h) Include COMSEC material, equipment, and surveillance requirements in USEUCOM operations and exercise plans and reviews component command supporting plans to ensure adequate COMSEC support requirements are identified and programmed.

(i) In support of OPSEC, promote the exchange of IA information and procedures among theater commands and IA activities.

(j) Identify anticipated fiscal year communications security surveillance requirements involving component command support of joint activities.

(k) Act as primary liaison with ECJ3 for matters relating to COMSEC support and communications-oriented cryptographic material in support of the USEUCOM OPSEC program.

(6) The Director of Public Affairs (ECPA) will:

(a) Ensure all public information releases and web-based content are developed in accordance with OPSEC guidance.

(b) Ensure all web masters receive OPSEC training prior to publishing any EUCOM online content.

(7) The USEUCOM Command Security Manager, on behalf of the Special Assistant for Security Matters (ECSM), will work with ECJ39 to:

(a) Review and coordinate on all plans to determine whether appropriate OPSEC measures have been incorporated. Conduct comparative analyses between Operational Classification Guidance and Essential Elements of Friendly Information to ensure accuracy, consistency, and standardization throughout the entire planning process.

(b) Develop and conduct OPSEC training for Directorate/Special Staff Security Managers.

(8) The USEUCOM Inspector General (ECIG) will:

(a) Schedule inspections of OPSEC programs in the annual IG Command Inspection Program.

(b) Inspect the HQ USEUCOM OPSEC program at least once every two years.

(c) Include OPSEC as a part of all inspections.

(d) Provide information on OPSEC inspection trends to the EOCG.

(e) Serve as a non-voting member of the EOCG.

(9) All HQ USEUCOM Directors will:

(a) Comply with OPSEC policy as stated herein.

(b) Develop and maintain an OPSEC Program.

(c) Appoint sufficient OPSEC officers to conduct a viable directorate OPSEC program, and identify individuals' names to ECJ39. OPSEC Officers will attend OPSEC Officer training provided by ECJ39.

(d) Develop and maintain critical information lists, and review them annually or as operations require.

(e) Develop OPSEC annexes/guidance for plans or activities over which primary staff responsibility is held, and contribute OPSEC guidance to plans/activities for which collateral responsibility is held.

(f) Support/conduct OPSEC surveys/OSEs as required.

(g) Provide newly assigned personnel (military and civilian) with an OPSEC awareness orientation within 60 days of arrival and with OPSEC reorientation training annually.

b. Component Commanders and JTF Commanders will:

(1) Comply with OPSEC policies established by this and service directives. Conflicts between this and service directives will be identified to HQ USEUCOM ECJ39.

(2) Establish and maintain an OPSEC program.

(3) Designate an OPSEC officer within the operations staff to be the focal point for OPSEC. Ensure the officer has a TOP SECRET clearance and access to Sensitive Compartmented Information (SCI) to facilitate effective liaison with EUCOM OPSEC personnel. Provide the names of command OPSEC officers to HQ USEUCOM ECJ39

(4) Develop and maintain critical information lists, and review them annually or as operations require.

(5) Establish OPSEC training programs to ensure that all personnel are familiar with OPSEC critical information and measures.

(6) Establish and pursue component-oriented OPSEC objectives.

(7) Provide guidance and assistance to subordinate organizations during the preparation of operations/contingency/exercise plans to ensure optimum consideration of OPSEC.

(8) Conduct OPSEC surveys/evaluations in accordance with this and service directives.

(9) Ensure all public information releases and web-based content are developed in accordance with OPSEC procedures.

(10) Provide an annual message report on the status of the component command OPSEC program to USCINCEUR, ATTN: ECJ39. The report will reflect status as of 30 June and arrive at this HQ NLT 31 July. The report will contain the following data:

- (a) Overview of OPSEC program status.
- (b) Training/indoctrination program activities.
- (c) OPSEC surveys conducted during the reporting periods, to include a summary of survey findings.
- (d) Lessons learned.
- (e) Component command OPSEC objectives.
- (f) Forecast of OPSEC activities for next reporting period.

c. USEUCOM Offices of Defense Cooperation will:

- (1) Comply with OPSEC policies established by this directive.
- (2) Establish and administer a training program to ensure all personnel are familiar with OPSEC considerations and applications.
- (3) Conduct periodic OPSEC evaluation/reviews of activities.
- (4) Submit OPSEC Quicklook Reports, when appropriate, in accordance with this directive.
- (5) Designate an officer to be the focal point for OPSEC.

FOR THE COMMANDER IN CHIEF:

OFFICIAL:

DANIEL J. PETROSKY  
Lieutenant General, USA  
Chief Of Staff

DAVID R. ELLIS  
LTC, USA  
Adjutant General

Appendixes

A - Definitions

B - OPSEC Quicklook Reporting

C - Operations Security Survey

DISTRIBUTION:

P

## Appendix A

### Explanation of Terms

A-1. Operations Security (OPSEC). The protection of military operations and activities resulting from the identification and subsequent elimination or control of intelligence indicators susceptible to hostile exploitation.

A-2. Operations Security (OPSEC) Data base. A narrative and graphic identification of all events associated with planning and executing an operation or function, including documentation of all known enemy efforts to obtain prior knowledge or foreknowledge of an operation or types of operations.

A-3. Command, Control and Communications Countermeasures (C3CM). The integrated use of operations security (OPSEC), military deception, jamming, and physical destruction, supported by intelligence, to deny information to, influence, degrade, or destroy adversary C3 capabilities, and to protect friendly C3 against such actions.

A-4 Counterintelligence (CI). Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

A-5. Deception. Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests or to cause injurious delay in his decisions and operations.

A-6. Physical Security. That element of security which results from all physical measures necessary to safeguard classified equipment, material, and documents from access or observation by unauthorized persons.

A-7. Information Security. A system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information the protection of which is authorized by executive order or statute.

A-8. Information Operations. IO are actions taken to affect adversary information and information systems while defending one's own information and information systems.

A-9. Communications Security (COMSEC). The protection resulting from the application of cryptosecurity, transmission security, and emission security measures to telecommunications and from application of physical security measures to COMSEC information. These measures are taken to deny

unauthorized persons information. These measures are taken to deny unauthorized study of such telecommunications or to ensure authenticity of such telecommunications.

A-10. Electronics Security (ELSEC). The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the interception and study of non-communications electromagnetic radiations (e.g., radar).

A-11. Signals Security (SIGSEC). A generic term which includes both COMSEC and ELSEC.

A-12. OPSEC Survey. A methodology used to determine the degree of protection afforded to a given operation or function, characterized by multiple functional outlines to identify all possible sources of information disclosure. Appendix III of this directive provides expanded discussion of the survey.

A-13. Operations Security Evaluation (OSE). An alternate survey methodology tailored to individual security-sensitive organization requirements where the organization is vulnerable to the all-source hostile threat and requires a sophisticated but focused threat assessment and/or vulnerability analysis.

A-14. Essential Elements of Friendly Information (EEFI). Aspects of information relating to planning, to an operation, or to a weapon system requiring protection. EEFI may take the form of questions or the form of positive statements. In either case, an EEFI listing should identify the duration of required protection and identify from whom the information should be protected. References b and c provide expanded guidance on EEFI development.

## Appendix B

## OPSEC Quicklook Reporting

B-1. Discussion. Personnel who have been adequately trained in OPSEC doctrine and application will be able to detect procedures detrimental to unit OPSEC posture as a matter of routine. This function should automatically take place in normal daily activities and operations, during special or atypical operations, and in the course of reviews and assessments of operations in which the unit has been previously engaged. If an OPSEC vulnerability is detected, a Quicklook Report is encouraged to alert others to problems identified. Procedures detrimental to OPSEC detected during a special operation or exercise for which a post exercise report is already required should include these OPSEC deficiencies as part of the report. OPSEC Quicklook reporting affords individual commands the opportunity to review their OPSEC posture using organic resources, and provides lessons learned to other military commanders. By definition, OPSEC Quicklook Reports are entirely voluntary; however, all commanders should encourage their submission. Quicklook Reports provide a means of improving military operational effectiveness based on the experience of other commanders. Reports should be given widest distribution.

B-2. Report Format. OPSEC Quicklook Reports should contain the following types of information:

- a. Explanation of the problem(s).
- b. Evaluation of the promulgated EEFI, if any. The evaluation should consider whether the EEFI were specific and comprehensive enough to alert personnel to the sensitive aspects of the operation.
- c. Evaluation of operational guidance. Was guidance based on EEFI and knowledge of the hostile threat? Was it helpful in avoiding disclosure of sensitive information?
- d. Recommendations for further developing/refining EEFI.
- e. Recommendations for changes to operational guidance and countermeasures such as procedural/tactical changes, equipment modifications, and OPSEC initiatives to reduce or eliminate the problem(s).

B-3. Report Distribution. Quicklook Reports should be distributed via the operational chain of command within the component commands of USEUCOM. Component command headquarters will forward copies of Quicklook Reports warranting intercomponent attention to HQ USEUCOM/ECJ39, and other component command headquarters as appropriate.

B-4. Utility. An OPSEC Quicklook Report, or a series of similar Quicklook Reports, may point out an especially significant, persistent, or widespread deficiency in the OPSEC measures which are

being applied to a particular operation or activity. Additionally, there may be indications that an enemy or potential enemy is exploiting certain unknown OPSEC weaknesses which are rendering an operation or mission unsuccessful, compromising the results of an R&D project, or disclosing intentions, capabilities, and tactics during the course of an exercise. If such is the case, an OPSEC survey may be in order.

## Appendix C

## Operations Security Survey

C-1. Discussion. Operations Security (OPSEC) surveys offer one method for evaluating the adequacy of security measures applied to a specific operation or task. Such surveys are normally conducted by teams composed of representatives from the various functional staff elements that may be participating in the operation or task. Reference c provides guidance on planning the accomplishment of an OPSEC survey. The following paragraph, with its subparagraphs, broadly defines an OPSEC survey and identifies functional aspects of the survey. Findings of OPSEC surveys are intended for use by commanders in improving the operational security and, consequently, the effectiveness of their commands.

C-2. OPSEC Survey. A methodology used to determine the degree of protection afforded to a given operation or function, characterized by multiple functional outlines to identify all possible sources of information disclosure. Functional outlines include:

- a. Communications. An identification of who talks to whom, what is transmitted, how the transmission is made, and when it occurs in relation to the planning and execution of an operation.
- b. COMSEC. An identification of all COMSEC measures and material available for a given operation, system, or organization and a determination of the amount and type of use of those measures and materials.
- c. Electromagnetic. An identification of electromagnetic emitters associated with an operation and function, including their deployment, probable emission patterns, and times of activation in relation to significant events of an operation or function.
- d. ELSEC. An identification of all ELSEC measures and material available for a given operation or system, and a determination of the amount and type of use of those measures and materials.
- e. Intelligence Threat. An identification of all known and possible enemy capabilities to collect and exploit information from a given or similar operation. This threat would include known enemy intelligence collection and analysis capabilities, efforts, and successes. An integral part of this process is a comprehensive assessment of enemy human intelligence (HUMINT), imagery intelligence (IMINT), signals intelligence (SIGINT), measures and signature intelligence (MASINT), and open source intelligence (OSINT) capabilities, to include land, air, sea, and space-based collection.
- f. Operations. An identification of all entities participating in an operation, their actions, and the time those actions occur in planning and executing an operation or function. It also includes identification of procedures used in the conduct and support of operations to ascertain whether stereotyped, predictable procedures are employed.

| g. Physical Security. An assessment of all physical security measures taken to safeguard classified equipment, material, and documents from access or observation by unauthorized persons.

| h. Supplementary Data. An identification of support function relating to or supporting operations (e.g., logistics, personnel, administration, etc.).

| C-3. Reporting. Reference c (Annex E) contains the suggested OPSEC survey reporting format.