

HEADQUARTERS
UNITED STATES EUROPEAN COMMAND
UNIT 30400
APO AE 09131

STAFF MEMORANDUM
NUMBER 40-2

4 June 2001

INTELLIGENCE

Oversight of Intelligence Activities

1. **Summary.** To establish policies, procedures and responsibilities for the oversight of intelligence activities within HQ USEUCOM.
2. **Applicability.**
 - a. This Directive applies to all intelligence activities in USEUCOM. It applies to all USEUCOM staff elements with intelligence activities; all joint task forces; all subordinate joint commands; Special Operations Command, Europe (SOCEUR); the Joint Analysis Center (JAC); and subordinate National Intelligence Centers (NIC).
 - b. This directive does not apply to the intelligence activities of USEUCOM component commands. Oversight activities of the component commands are conducted and reported to their services under service regulations.
3. **Internal Control System.** This Directive contains internal control provisions and is subject to the requirements of the internal management control program. For HQ USEUCOM and subordinate joint organizations, the applicable internal control directive is ED 50-8, Internal Management Control Program.
4. **Suggested Improvements.** Staff proponent for this Directive is ECJ2-SSO, Intelligence Directorate. Forward suggested improvements to HQ USEUCOM, ATTN: ECJ2-SSO, Unit 30400, APO AE 09131.
5. **References.**
 - a. Executive Order 12333, "United States Intelligence Activities."
 - b. DoD Directive 5200.26, "Defense Investigative Program."
 - c. DoD Directive 5240.1, "DoD Intelligence Activities."
 - d. DoD Regulation 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons."

- e. Joint Chiefs Of Staff (JCS) MCM-75-91, "Oversight of Intelligence Activities."
 - f. CJCSI 5901.01, "Conduct of Inspections, Investigations, and Intelligence Oversight."
 - g. EUCOM Directive (ED) 125-4, "The USEUCOM Inspector General."
 - h. Army Regulation 381-10, "US Army Intelligence Activities."
6. **Definition of Terms**. See Appendix A.
7. **Responsibilities**.
- a. USEUCOM Directorate of Intelligence (ECJ2) will:
 - (1) Appoint an IO Officer and IO Training Officer for USEUCOM (one person may fill both positions). This person or persons will direct the USEUCOM IO Program IAW with this directive and its references.
 - (2) Formulate all policy and procedural guidance on IO compliance for USEUCOM ECJ2 and subordinate joint intelligence organizations (excepting the components) IAW references a-h.
 - (3) Develop an IO training program and ensure it is effectively implemented, maintained, and documented by all ECJ2 divisions and subordinate joint intelligence activities.
 - (4) Develop an IO self-inspection program and ensure it is effectively implemented, maintained, and documented by ECJ2 divisions and subordinate joint intelligence activities.
 - (5) Provide ECIG the name, phone number and title of individuals for each USEUCOM intelligence activity (except the components) who are appointed to IO Officer and Training Officer positions. Include updates of this list with each quarterly report to ECIG.
 - (6) Provide quarterly IO activity reports to ECIG who consolidates inputs from all intelligence activities. Submit the reports NLT five working days after the end of each quarter ending the last work day of DEC, MAR, JUN, and SEP. Reports will follow the format at appendix C. Negative reports are required.
 - b. USEUCOM Inspector General (ECIG) will:
 - (1) Monitor, inspect, assess, and evaluate Intelligence Oversight (IO) activities. Conduct at least one intelligence oversight inspection quarterly.
 - (2) Coordinate selection of activities for intelligence oversight inspections with ECJ2.

(3) Ensure procedures exist for reporting questionable activities and that personnel are aware of their responsibilities for reporting such activity. Include review or inspection of other areas in conjunction with IO activity inspections as directed by CINCEUR.

(4) Report inspection results to the DCINCEUR; recommend actions to correct deficiencies or to improve inspections and monitoring of the theater IO Inspection Program.

(5) Report any questionable intelligence activity immediately to the Joint Staff IG on behalf of USCINCEUR.

(6) Prepare and submit quarterly IO activity report to the Joint Staff IG NLT 15 working days after the close of each quarter ending on the last work day of DEC, MAR, JUN and SEP. Negative reports are required. Report will include information as shown in the report format at enclosure/appendix C.

c. USEUCOM Staff Judge Advocate (ECJA) will:

(1) Provide legal interpretation of references a-h, legal advice, and assistance concerning IO issues.

(2) Provide releasability review of information requested for release by other agencies normally provided for under procedure four of ref e.

(3) Report to ECIG, no later than 10 working days after the end of a quarter, any information received regarding questionable intelligence activities. Negative reports are required.

d. USEUCOM staff representatives and subordinate joint intelligence organizations will:

(1) Appoint in writing an IO Officer and Training Officer responsible for managing the IO Program within their division or subordinate joint intelligence activity and for coordinating and reporting on IO matters with the USEUCOM IO Officer.

(2) Conduct IO training.

(a) Each IO Officer will conduct initial IO training of all personnel within 30 days of their arrival at the activity. (See Appendix D) Initial training will emphasize Procedures 1-4, 14 and 15 of DoD 5240.1-R (Appendix G). Initial training will be documented by using Acknowledgement Statements. These statements will be made available to inspectors. Initial IO training will be reflected in the quarterly reports.

(b) At HQ USEUCOM, annual refresher training will be conducted and documented by the HQ USEUCOM IO Officer. Annual training at HQ USEUCOM and other intelligence activities must be documented in such a way as to clearly show inspectors that the training was conducted and that all activity personnel received the training.

(3) Conduct Self-Inspection. All USEUCOM intelligence activities will conduct quarterly self-inspections. These self-inspections will follow the format shown at appendix C and will include files review of administrative files, computer files, intelligence files, and databases. The self-inspection will include interviews of twenty-five percent of personnel assigned to the activity to ensure determine if personnel remain aware of IO and their responsibilities. IO Self-Inspection results will be reported in quarterly reports. (See Appendix B) for an example of self-inspection.

(4) Subordinate intelligence activities will submit quarterly IO reports to the USEUCOM IO Officer NLT the first work day after the end of the quarter. (See Appendix C) for example of a quarterly report.

(5) Report IO incidents. All IO representatives are responsible to investigate and report IO incidents or suspected incidents to the USEUCOM IO Officer as they are discovered. IO representatives will investigate the matter internally, collecting the material in question, interviewing persons involved and determining the reason for obtaining, processing and retaining the material. IO representatives will forward a complete report of the findings to the USEUCOM IO Officer within five working days of incident's discovery. (APPENDIX F)

FOR THE COMMANDER IN CHIEF

OFFICIAL:

DANIEL J. PETROSKY
Lieutenant General, US Army
Chief of Staff

DAVID R. ELLIS
LTC, USA
Adjutant General

DISTRIBUTION
P

APPENDIXES:

A - Explanation of Terms
B - IO Quarterly Self Inspection
C - IO Quarterly Report
D - IO Activities Training
E - IO Training Book
F - IO Incident Reporting
G - IO Procedures

APPENDIX A

Explanation of Terms

A-1. **US PERSONS:** A US Person is defined as a citizen of the United States; an alien known by the intelligence agency concerned to be a permanent resident alien; an unincorporated association organized in the United States or substantially composed of US citizens or permanent resident aliens; or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

A-2. **QUESTIONABLE ACTIVITY:** Any intelligence collection activity not conducted pursuant to and in accordance with Executive Order 12333 and DoD regulations.

A-3. **COLLECTION:** Information shall be considered as “collected” only when it has been received for use by an employee of a DoD intelligence component in the course of his/her official duties. Thus, information volunteered to a DoD intelligence component by a cooperating source would be “collected” under this procedure when an employee of such component officially accepts, in some manner, such information for use within that component. Data acquired electronically means “collected” only when it has been processed into an intelligence form.

A-4. **COOPERATING SOURCE:** Persons or organizations that knowingly and voluntarily provide information to DoD intelligence components, or access to information, at the request of such components or their own initiative. They include government agencies, law enforcement authorities, credit agencies, academic institutions and foreign governments.

A-5. **ADMINISTRATIVE PURPOSE:** Information is collected for administrative purposes when it is necessary for the administration of the component concerned but is not collected directly in performance of the intelligence activities. Examples include information relating to past performance of potential contractors; information to enable such components discharge their public affairs and legislative duties; employee training and personnel records.

A-6. **AVAILABLE PUBLICLY:** Information that has been published or broadcast for the general public consumption, is available on request to a member of the general public, could lawfully be seen or heard by any casual observer, or is made available at a meeting open to the general public. In this context, the general public also means general availability to persons in a military community even though the military community is not open to the civilian general public.

ANNEX B

IO Quarterly Self-Inspections

1. Each IO representative is responsible for conducting quarterly self-inspections of their respective divisions.
2. At a minimum 25 percent of the activity's files and databases will be reviewed for compliance with IO. The intelligence oversight representative will inspect intelligence files and databases for any information that contains information regarding to U.S. persons. This includes biographical information, names, SSANs, and any other detailed information about U.S. persons.
3. Personnel Interviews: Five percent of activity personnel will be selected at random and questioned on their knowledge of IO. Persons questioned should be familiar with:
 - a. Definition of a U.S. Person
 - b. Purpose of Intelligence Oversight
 - c. What is questionable activity
 - d. IO reporting chain
 - e. Who is the EUCOM IO Office and unit IO Representative
 - f. Procedures 1-4, 14, 15.
4. Files review: Inspect 25 percent of files maintained in the organization for IO compliance. This includes all administrative files, logistic files, computer files and intelligence files. IO representatives will ensure that no files contain information on U.S. persons that are being used for intelligence purposes without having proper authorization or justification these files. In addition to files review each representative will review individual intelligence oversight training files to ensure their personnel are up to date with intelligence oversight training requirements.

APPENDIX C

IO Quarterly Report

1. Each IO representative must provide a quarterly report NLT 1 working day at the end of the quarter. The quarterly report will consist of the following:
 - a. Number of personnel receiving initial briefing.
 - b. Number of personnel receiving refresher training.
 - c. Number of personnel questioned regarding IO knowledge.
 - d. What files were reviewed and results of the review.
 - e. IO incidents during the quarter.
 - f. Name and phone number of IO representative.
2. The following is an example of an IO Quarterly Report.

ECJ2-SSO

Date

MEMORANDUM FOR EUCOM Intelligence Oversight Officer

SUBJECT: 1st Qtr FY 00 IO Report

1. The following IO information is provided for (*your division, i.e. J25, J23 etc*)
 - a. Activity IO representative:
 - b. Activity IO representative phone #:
 - c. Number of initial briefings:
 - d. Number of refresher briefings:
 - e. Number of personnel interviewed:
 - f. Description of files reviewed: (*A 25% review of computer files revealed no information was retained which violated any Intelligence Oversight Procedures*)

APPENDIX C (Cont)

IO Quarterly Report

- g. Number and description of any IO incidents:
- 2. POC (Name, Office symbol and phone number)

Signature Block

APPENDIX E

Intelligence Oversight Book

1. All IO representatives will maintain an IO book. The book may be a binder, a file, or it may be formatted to best suit the individual user. However, the following material at a minimum is included in the book:

- a. **Appointment Orders:** Appointment orders for the IO officer and training officer.
- b. **Directives and Regulations:** All regulations and directives reference in this Directive shall be maintained in this book or will be readily accessible via the Internet or CD-ROM.
- c. **IO Acknowledgement Statements:** All acknowledgement statements for all assigned personnel attesting that they have been briefed and understand IO policy and procedures.
- d. **Quarterly IO Reports:** A copy of each quarterly report going back two years.

APPENDIX F

Intelligence Oversight Incident Reporting

1. All individuals are required to report intelligence oversight incidents/questionable activities to their activity IO representative, EUCOM IO Officer, or EUCOM IG upon discovery of the incident or questionable activity.
2. IO representatives will provide a complete report of findings to the USEUCOM IO Officer within five working days of incident's discovery. This report can be done in a memorandum format.
3. Failure to report IO violations or questionable activity is in itself a violation of IO policies.

APPENDIX G

Intelligence Oversight Procedures

All personnel assigned to intelligence directorates and subordinate joint intelligence organizations at a minimum must know the following procedures:

1. **Procedure 1:** General Provisions: Outlines responsibilities of the DoD manual and defines who the DoD regulations apply to as well as defining terms associated with intelligence collection and information.
2. **Procedure 2:** Collection of Information about U.S. Persons. Specifies the kinds of information about U.S. persons that may be collected by DoD intelligence components and sets forth general criteria governing the means used to collect such information. Additional limitations are imposed in Procedures 5-10 on the use of specific techniques.

Types of information that may be collected about U.S. persons.

- a. Information obtained with consent.
- b. Publicly available information
- c. Foreign Intelligence information about a U.S. person may be collected provided the following is met:
 - (1) Individuals believed to be officers or employees or otherwise acting for or on behalf, of a foreign government.
 - (2) An organization reasonably believed to be owned or controlled directly or indirectly by a foreign power.
 - (3) Persons or organizations reasonably believed to be engaged or about to engage in international terrorist or international narcotics activity.
 - (4) Corporations or other commercial organizations believed to have some relationship with a foreign power, organizations or persons.
- d. Potential sources of assistance to intelligence activities. Information may be collected about U.S. persons reasonably believed to be potential sources of intelligence.
- e. Information may be collected about U.S. persons who threaten the physical security of DoD employees, installations, operations or official visitors.

APPENDIX G (CONT)

Means by which information may be collected about U.S. persons.

1. Least intrusive means: Whenever possible information shall be collected utilizing public available information or information obtained with consent of individual.

c. **Procedure 3:** Retention of Information about U.S. Persons. Pertains to information retained by a DoD intelligence organization for the use as intelligence. This does not include information that is used for administrative purposes.

(1) Information collected pursuant to procedure 2 may be retained.

(2) Temporary Retention: Information may be retained about U.S. persons for a period not to exceed 90 days, solely for the purposes of determining whether that information may be permanently retained under these procedures.

d. **Procedure 4:** Dissemination of Information about U.S. Persons

Criteria for Dissemination: Information about U.S. persons that identifies those persons may be disseminated without the consent of those persons only under the following conditions:

(1) Information was collected or retained or both under Procedures 2 & 3.

(2) The recipient is reasonably believed to have a need to receive such information for the performance of a lawful governmental function, and is one of the following:

a. An employee of DoD, or an employee of a contractor of DoD, and has a need for such information in the course of his/her official duties.

b. A law enforcement entity of the federal, state or local government, and the information may indicate involvement in activities which may violate laws which the recipient is responsible to enforce.

c. An agency within the intelligence community; provided that within the intelligence community, information other than information derived from signals intelligence, may be disseminated to each appropriate agency for the purpose of allowing the recipient agency to determine whether the information is relevant to its responsibilities without such a determination being required of the disseminating DoD intelligence component.

APPENDIX G (CONT.)

d. An agency of the federal government authorized to receive such information in the performance of a lawful governmental function.

e. A foreign government and dissemination is undertaken pursuant to an agreement or other understanding with such government.

e. **Procedure 14:** Employee conduct

1. Employee responsibilities: Employees shall conduct intelligence activities only pursuant to, and in accordance with, Executive Order 12333 and DoD 5240.1-R. In conducting such activities, employees shall not exceed the authorities granted the employing DoD intelligence component by Law, Executive Order, including Executive Order 12333 and applicable DoD regulations.

f. **Procedure 15:** Identifying, Investigating and Reporting Questionable Activities

1. All employees assigned to a DoD intelligence component must report questionable activity to their respective IO Officer or Inspector General. Questionable activity refers to any activity that may violate the law or Executive Order 12333.