

July 7, 1983
NUMBER 5205.2

USDP

Department of Defense Directive

SUBJECT: DoD Operations Security Program

- REFERENCES:
- (a) DoD Directive 5130.2, "Director of Policy Review," June 16, 1977
 - (b) DoD Directive 5105.42, "Defense Investigative Service (DIS)," July 19, 1978
 - (c) DoD Directive 5400.7, "DoD Freedom of Information Act Program," March 24, 1980
 - (d) JCS Pub 18, "Operations Security," December 15, 1982
 - (e) DoD Directive 5220.22, "DoD Industrial Security Program," December 8, 1980
 - (f) DoD 5220.22-R, "Industrial Security Regulation," January 1983, authorized by reference (e)

A. PURPOSE

This Directive establishes the DoD operations security (OPSEC) program, provides policy, and assigns responsibilities.

B. APPLICABILITY

1. This Directive applies to the Office of the Secretary of Defense, the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, and the Defense Agencies (hereafter referred to collectively as "DoD Components").

2. The DoD OPSEC program shall be applied to DoD contractors participating in the DoD Industrial Security Program when the DoD Component concerned has determined that such measures are essential for the adequate protection of classified information with respect to a specific classified contract.

C. DEFINITION

Operations Security. The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities.

93-26889

4px

D. POLICY

1. It is the policy of the Department of Defense that each DoD Component shall establish an OPSEC program. This program shall ensure the protection of DoD programs, operations, and activities, balancing mission effectiveness if essential secrecy is not preserved against costs of maintaining essential secrecy.

2. DoD mission effectiveness depends on keeping classified information secret.

a. The necessary condition for maintaining essential secrecy is protection of classified materials. However, such protection is not always adequate because adversaries monitor open sources and detectable activities to derive indicators of U.S. intentions, capabilities, and current activities. Although unclassified, the information thus gained has intelligence value and is used to prepare estimates about uncertainties and unknowns. If accurate, these estimates may have the same effect as the direct compromise of classified information.

b. The sufficient condition for essential secrecy is therefore use of OPSEC, supported as necessary by military deception, to deny indicators to adversaries.

E. RESPONSIBILITIES

1. The Deputy Under Secretary of Defense for Policy (DUSD(P)) under authority established in DoD Directive 5130.2 (reference (a)), shall:

a. Establish policies for the conduct of the DoD OPSEC program.

b. Provide for oversight of DoD Components' OPSEC programs.

c. As requested, coordinate relations of DoD Components with other governmental agencies on OPSEC matters.

d. As requested, coordinate OPSEC matters affecting more than one DoD Component.

2. Heads of DoD Components shall:

a. Establish an OPSEC program. At a minimum this program shall include OPSEC training, OPSEC surveys as appropriate, and use of OPSEC in planning.

b. Provide support for OPSEC programs of other DoD Components as necessary.

c. Provide management, review, and inspection of their OPSEC programs.

d. Recommend to the DUSD(P) changes to policies, procedures, or practices of the DoD OPSEC program.

e. Determine if OPSEC measures are required of a DoD contractor for performance of a classified contract. If so, ensure that such measures are incorporated specifically into the request for proposal and resultant contract documents in sufficient detail to enable cost reimbursement of and program compliance by the contractor.

f. Provide details of OPSEC measures as determined in paragraph E.2.e., above, to the cognizant security office of the Defense Investigative Service (reference (b)) for management, review, and inspection at contractor facilities not located on military installations.

g. Provide assistance to the Defense Investigative Service to ensure adequacy of industrial security inspection efforts relating to OPSEC measures as defined in paragraph E.2.e., above.

h. Ensure that measures taken to implement the DoD OPSEC program are in compliance with the Freedom of Information Act (reference (c)).

3. The Joint Chiefs of Staff, in addition to the tasks specified in subsection E.2., above, shall:

a. Maintain authority, direction, and control of the JCS OPSEC program (reference (d)).

b. Establish OPSEC requirements and procedures for the Unified and Specified Commands.

c. Establish OPSEC requirements for DoD Components as appropriate for use in preparation of strategic plans and joint logistic plans.

d. Publish OPSEC documents for use by the Unified and Specified Commands and other DoD Components in their OPSEC programs.

e. Determine OPSEC requirements necessary for effective military operations that must be implemented by non-DoD agencies.

4. The Director, Defense Investigative Service, in addition to the tasks specified in subsection E.2., above, shall:

a. Inspect DoD contractors, in conjunction with representatives of the DoD Component if requested by the Component, for compliance with contractually incorporated OPSEC measures (paragraph E.2.e., above) during scheduled security inspections performed under DoD Directive 5220.22 and DoD 5220.22-R (references (e) and (f)) or as requested by DoD Components. On military installations such inspections will be performed only when requested by the installation commander.

b. Coordinate DoD Component visits to contractors as part of established industrial OPSEC programs.

c. Request assistance as necessary from the appropriate DoD Component to conduct inspections as required by paragraph E.4.a., above.

d. Incorporate OPSEC concepts, planning procedures, and survey guidance in DIS training courses and pertinent DIS directives.

Jul 7, 83

5205.2

5. The Director, National Security Agency/Chief, Central Security Service, in addition to the tasks specified in subsection E.2., above, shall collaborate with the heads of the DoD Components in providing COMSEC support for OPSEC surveys.

F. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward one copy of implementing documents to the Deputy Under Secretary of Defense for Policy within 120 Days.

PAUL THAYER
Deputy Secretary of Defense

Accession For

NTIS

DTIC

U.S. GOVERNMENT

per form D

By

Date

6-1

DTIC QUALITY INSPECTED 8