



Department of Defense DIRECTIVE

NUMBER 5205.2

November 29, 1999

ASD(C3I)

SUBJECT: DoD Operations Security (OPSEC) Program

- References:
- (a) DoD Directive 5205.2, "DoD Operations Security Program," July 7, 1983 (hereby canceled)
 - (b) National Security Decision Directive (NSDD) No. 298, "National Operations Security Program," January 22, 1988
 - (c) [DoD Directive 5100.20](#), "The National Security Agency and the Central Security Service," December 23, 1971
 - (d) [DoD Directive 5200.39](#), "Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection," September 10, 1997
 - (e) through (h), see enclosure 1

1. REISSUANCE AND PURPOSE

This Directive:

1.1. Reissues reference (a) to update policy and responsibilities governing the DoD Operations Security (OPSEC) Program, and incorporates the requirements of reference (b) that apply to the Department of Defense.

1.2. Designates the Director, National Security Agency as the "DoD Executive Agent" for inter-Agency OPSEC training (references (b) and (c)).

2. APPLICABILITY AND SCOPE

This Directive:

2.1. Applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Defense Agencies, and the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Components").

2.2. Ensures that OPSEC planning and analysis, to determine applicability, is performed by those most familiar with the operational aspects of a particular activity together with their supporting intelligence, counterintelligence, and security countermeasures elements. The applicability, implementation, scope, and OPSEC measures are determined by commanders, supervisors, or decision-makers with the ultimate responsibility for mission accomplishment.

2.3. Applies to all activities that prepare, sustain, or employ the U.S. Armed Forces during war, crisis, or peace. The DoD OPSEC Program reaches all levels of military operations; research, development, test and evaluation activities; treaty verification activities, nonproliferation protocols, and international agreements; and other selected support activities such as force protection.

2.4. Applies to DoD contracts that support the functions stated in paragraph 2.3., above when the Heads of the DoD Components, or their designated representative, determine, in writing, that OPSEC measures are necessary in a contract. Certain acquisition programs may require OPSEC measures to help protect critical program information in accordance with DoD Directive 5200.39 (reference (d)).

2.5. Applies to special access programs as they require unique OPSEC plans, surveys, and activities to be conducted as a method to identify, define, and provide countermeasures to vulnerabilities in accordance with DoD Directive O-5205.7, DoD Instruction O-5205.11, and DoD 5220.22-M (references (e), (f), and (g)).

2.6. The DoD Components with minimal activities that could affect national security may apply to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence for an exemption to the requirement to establish a formal OPSEC program.

3. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

4. POLICY

It is DoD policy that:

4.1. National security-related missions or functions shall have an OPSEC program incorporating the common features listed in paragraph 5.2., below, and the Heads of the DoD Components shall apply sound risk management principles when allocating resources to mitigate threats.

4.2. Extraordinary protection of DoD acquisition programs, defense activities, or military operations and their attendant costs for maintaining essential secrecy through the OPSEC process are balanced against the potential loss to mission effectiveness.

4.3. The essential secrecy of information critical to adversaries in their planning, preparing, and conducting military and other operations against the United States be maintained.

4.3.1. A necessary condition for maintaining essential secrecy is protection of classified and unclassified critical information ensuring that besides the application of traditional security measures, the Department of Defense maintains a heightened awareness of potential threats of adversaries taking advantage of publicly available information and other detectable unclassified activities to derive indicators of U.S. intentions, capabilities, operations, and activities.

4.3.2. The OPSEC analytic process is based on the identification and mitigation of these indicators.

4.3.3. OPSEC countermeasures shall be employed to deny indicators to adversaries that reveal critical information about the Department of Defense and U.S. missions and functions.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence shall:

5.1.1. Establish policies for the conduct of DoD OPSEC programs.

5.1.2. Provide for periodic review of the DoD OPSEC program.

5.1.3. Coordinate relations of the DoD Components with the other Government Agencies on OPSEC matters.

5.1.4. When applicable, advise the National Security Council (NSC), through the Secretary of Defense, on OPSEC countermeasures required of the other Executive Departments and Agencies to achieve and maintain effective operations or activities.

5.1.5. Coordinate OPSEC matters affecting more than one DoD Component.

5.1.6. In coordination with the acquisition community, develop standards and procedures for the evaluation and protection, when necessary, of unclassified contract efforts.

5.1.7. Ensure that OPSEC is an integral element in the development and implementation of information operations strategies.

5.1.8. Ensure the assignment of representatives from the Department of Defense to the Inter-Agency OPSEC Support Staff (IOSS), as required by reference (b).

5.1.9. Ensure the Director, Defense Intelligence Agency, besides the tasks specified in paragraph 5.2., below, shall provide intelligence and counterintelligence threat analysis to support OPSEC planning to all DoD Components that submit validated production requirements.

5.1.10. Ensure the Director, Defense Security Service, besides the tasks specified in paragraph 5.2., below, shall:

5.1.10.1. Ensure compliance with OPSEC requirements incorporated in classified contracts during scheduled security reviews performed under the National Industrial Security Program (NISP). If required, ensure that the specific threats and OPSEC measures are identified that shall protect the critical or sensitive information. On military installations, such inspections shall be performed only when requested by the installation commander.

5.1.10.2. Request assistance, as necessary, from the applicable DoD Component to conduct inspections required by subparagraph 5.1.10.1., above.

5.1.10.3. When requested, coordinate with and assist user Agencies in OPSEC surveys for contractors performing classified contracts and participating in the NISP.

5.2. The Heads of the DoD Components shall:

5.2.1. Establish an OPSEC program, in accordance with NSDD 298 (reference (b)) that, at a minimum, shall include:

5.2.1.1. Assignment of responsibility for OPSEC direction and implementation.

5.2.1.2. Issuance of procedures and planning guidance for the use of OPSEC techniques to identify vulnerabilities and apply applicable countermeasures.

5.2.1.3. Establishment of OPSEC education and awareness training.

5.2.1.4. Annual review and validation of OPSEC plans and programs.

5.2.2. Provide support for OPSEC programs of the other DoD Components, as necessary.

5.2.3. Provide management, annual review, and evaluation of their OPSEC programs.

5.2.4. Ensure that OPSEC requirements are included in contracts, when applicable.

5.2.5. Provide assistance to the Defense Security Service for ensuring adequacy of industrial security efforts for OPSEC countermeasures, if required under section 2., above, for classified contracts.

5.3. The Chairman of the Joint Chiefs of Staff shall:

5.3.1. Provide guidance to the Commanders of the Combatant Commands for their annual review and evaluation of their OPSEC programs.

5.3.2. Determine OPSEC requirements necessary for effective military operations that must be implemented by non-DoD Agencies (Joint Pub 3-54, reference (h)). Advise the NSC through the OSD of the impact of nonmilitary U.S. policies on the effectiveness of OPSEC measures taken by the Armed Forces, and recommend to the NSC policies that minimize any adverse effects.

5.4. The Director, National Security Agency, in addition to the tasks specified in paragraph 5.2., above, and as directed by NSDD 298 (reference (b)), shall act as the DoD Executive Agent for inter-Agency OPSEC training, with responsibility to:

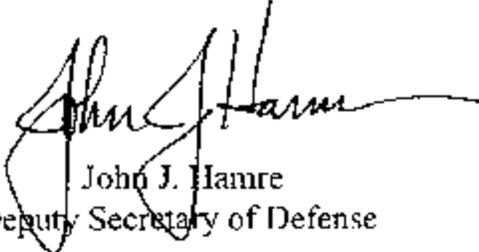
5.4.1. Assist Executive Departments and Agencies, as needed, in establishing OPSEC programs.

5.4.2. Develop and provide inter-Agency OPSEC training courses.

5.4.3. Establish and maintain an IOSS.

6. EFFECTIVE DATE

This Directive is effective immediately.



John J. Hamre
Deputy Secretary of Defense

Enclosures - 2

E1. References, continued

E2. Definitions

E1. ENCLOSURE 1

REFERENCES, continued

- (e) DoD Directive O-5205.7, "Special Access Program (SAP) Policy," January 13, 1997
- (f) DoD Instruction O-5205.11, "Management, Administration, and Oversight of DoD Special Access Programs (SAPs)," July 1, 1997
- (g) [DoD 5220.22-M](#), "National Industrial Security Program Operating Manual (NISPOM)," January 1995
- (h) Joint Pub 3-54, "Joint Doctrine for Operations Security," January 24, 1997

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Acquisition Program. A directed and funded effort that is designed to provide a new, improved, or continuing weapons system or automated information system capability in response to a validated operational need.

E2.1.2. Critical Information. Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively to guarantee failure or unacceptable consequences for friendly mission accomplishment.

E2.1.3. Critical Program Information (CPI). CPI, 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 unclassified controlled information about such programs, technologies, or systems.

E2.1.4. Essential Secrecy. The condition achieved from the denial of critical information to adversaries.

E2.1.5. Operations Security (OPSEC). For the DoD Components, OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to defense acquisition, defense activities, military operations, and other activities to:

E2.1.5.1. Identify those actions that may be observed by adversary intelligence systems.

E2.1.5.2. Determine what indicators hostile intelligence systems may obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

E2.1.5.3. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

E2.1.6. OPSEC Process

E2.1.6.1. The OPSEC process is an analytical, risk-based process that incorporates five distinct elements:

E2.1.6.1.1. Identifying critical information;

E2.1.6.1.2. Analyzing threats;

E2.1.6.1.3. Analyzing vulnerabilities;

E2.1.6.1.4. Assessing risks; and

E2.1.6.1.5. Applying countermeasures.

E2.1.6.2. The OPSEC process examines a complete activity to determine what, if any, exploitable evidence of classified or sensitive activity may be acquired by potential adversaries.