



Department of Defense

DIRECTIVE

NUMBER 5205.02

March 6, 2006

USD(I)

SUBJECT: DoD Operations Security (OPSEC) Program

References: (a) DoD Directive 5205.2, "DoD Operations Security Program," November 29, 1999 (hereby canceled)
(b) National Security Decision Directive (NSDD) No. 298, "National Operations Security Program," January 22, 1988¹
(c) DoD Directive S-3600.1, "Information Operations (IO) (U)," December 9, 1996²
(d) Joint Publication 1-02, "DoD Dictionary of Military and Associated Terms," April 12, 2001
(e) through (f), 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. Under Reference (b), designates the Director, National Security Agency as the Federal Executive Agent for interagency OPSEC training.

1.3. Underscores the importance of OPSEC and how it is integrated as a core military capability within Information Operations (IO) that must be followed in daily application of military operations (Reference (c)).

¹ Available at the following website: <http://www.ioss.gov/nsdd298.html>

² This Directive is classified as SECRET. Readers with the correct clearance may contact the POC listed at the website.

2. APPLICABILITY AND SCOPE

This Directive:

- 2.1. Applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the “DoD Components”).
- 2.2. Requires that OPSEC planning and analysis is performed by commanders, supervisors, or decision makers charged with the ultimate responsibility for mission accomplishment, i.e., those most familiar with the operational aspects of a particular activity including the supporting intelligence, counterintelligence, and security countermeasures.
- 2.3. Applies to all activities that prepare, sustain, or employ U.S. Armed Forces during war, crisis, or peace including such activities as those involving research, development, test and evaluation; DoD contracting; treaty verification; nonproliferation protocols; international agreements; force protection; and the release of information to the public. OPSEC is a core capability of IO, and as such, OPSEC supports land, sea, air, and space operations. The level of OPSEC to apply is dependent on the assigned mission and the circumstances, targets, and resources available.
- 2.4. Requires that the Heads of the DoD Components designate OPSEC Program Managers or Coordinators in all commands and agencies and establish and maintain an OPSEC program that promotes an understanding of OPSEC among all personnel. Additionally, ensures that OPSEC training and education is established and available to the IO career force personnel commensurate with their responsibilities.

3. DEFINITIONS

Terms used in this Directive are defined in Enclosure 2 and Joint Publication 1-02 (Reference (d)).

4. POLICY

It is DoD policy that:

- 4.1. National security-related missions and functions shall be protected by an OPSEC program. Risk management principles shall be applied to OPSEC programs when allocating resources to mitigate threats.

4.2. The OPSEC protection afforded to DoD acquisition programs, defense activities, or military operations shall be balanced with the potential loss to mission effectiveness and their attendant cost. OPSEC and security programs shall be closely coordinated to ensure that all aspects of sensitive operations and force protection are protected.

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

4.3.1. Adversary intelligence collection threats include the exploitation of publicly available information often obtained through open networks and information on websites. These and other detectable unclassified activities are used to derive indicators of U.S. intentions, capabilities, operations, and activities. A necessary condition for maintaining essential secrecy is protection of classified, as well as unclassified critical information. This protection ensures that, beyond the application of traditional security measures, the Department of Defense maintains a heightened awareness of potential threats.

4.3.2. The OPSEC analytic process is based on the identification and mitigation of these indicators of U.S. intentions, capabilities, operations, and activities.

4.3.3. OPSEC measures shall be employed to deny indicators to adversaries that reveal critical information about DoD missions and functions.

4.3.4. As an operations activity, OPSEC will be considered during the entire life-cycle of military operations or activities.

4.4. OPSEC is a core capability of IO. OPSEC capabilities shall be developed and employed in concert with other military and core IO capabilities to provide a fully integrated warfighting capability.

5. RESPONSIBILITIES

5.1. The Under Secretary of Defense for Intelligence (USD(I)) shall:

5.1.1. Establish and oversee the implementation of policies and procedures for the conduct of the DoD OPSEC Program, including monitoring, evaluating, and periodically reviewing all DoD OPSEC activities.

5.1.2. As the functional proponent for the IO career force, oversee specialized OPSEC training for the IO career force.

5.1.3. Report annually to the Secretary of Defense on the status of the DoD OPSEC Program.

5.1.4. Coordinate and deconflict OPSEC matters affecting more than one DoD Component and identify other U.S. Government department or agency policies that may adversely affect DoD OPSEC posture.

5.1.5. Develop and issue guidance regarding standards that must be met in conducting vulnerability assessments and OPSEC surveys.

5.1.6. In coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics, develop standards and procedures for the evaluation and protection, when necessary, of unclassified and classified contract efforts.

5.1.7. Assign DoD representatives to the Interagency OPSEC Support Staff (IOSS), as required by Reference (b).

5.2. The Under Secretary of Defense for Policy shall:

5.2.1. Coordinate international cooperation agreements involving the planning and execution of OPSEC.

5.2.2. Review all Combatant Commander operations and contingency plans to ensure OPSEC integration.

5.2.3. Integrate OPSEC measures into the DoD Critical Infrastructure Protection Program.

5.3. The Heads of the DoD Components shall:

5.3.1. Establish an OPSEC program focused on command involvement, assessments, surveys, training, education, threat, resourcing, and awareness that, at a minimum, includes:

5.3.1.1. Assignment of responsibilities for OPSEC direction and implementation, and provision for full-time OPSEC Program Managers or Coordinators at appropriate command levels.

5.3.1.2. Establishment of an OPSEC support capability that provides for program development, planning, training, assessment, surveys, and readiness training.

5.3.1.3. Issuance of procedures and planning guidance for the use of the OPSEC analytic process.

5.3.1.4. An annual review and validation of Component OPSEC programs, the results of which shall be submitted annually to the USD(I).

5.3.1.5. The conduct of OPSEC surveys for subordinate commands and agencies at least once every 3 years in order to enhance mission effectiveness.

5.3.1.6. Support for OPSEC programs to other DoD Components as necessary.

5.3.2. Issue guidance regarding the techniques, training, and procedures for conducting vulnerability assessments and OPSEC surveys.

5.3.3. Ensure adequate practices are in place to prevent adversaries from taking advantage of and aggregating publicly available information according to DoD Directive 5230.9, (Reference (e)) and other detectable unclassified activities to derive indicators of U.S. intentions, capabilities, operations, and activities.

5.3.4. Ensure that critical information is identified and updated as missions change, and coordinate OPSEC matters with other affected Government agencies when working in an interagency environment.

5.3.5. Ensure that OPSEC awareness, training and education are established and provided to OPSEC Program Managers or Coordinators, the IO career force and other DoD personnel commensurate with their respective responsibilities to ensure that OPSEC is integrated into all elements of training.

5.3.6. Ensure that the Government's contract requirements properly reflect OPSEC responsibilities and are included in contracts when applicable.

5.3.7. Provide assistance to the Defense Security Service for ensuring adequacy of industrial security efforts for OPSEC countermeasures for classified contracts.

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

5.4.1. Serve as the principal advisor to the President and the Secretary of Defense on all military OPSEC matters.

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

5.4.3. Determine OPSEC requirements necessary for effective military operations.

5.5. The Commanders of the Combatant Commands, through the Chairman of the Joint Chiefs of Staff, shall integrate OPSEC into all contingency planning and operations.

5.6. The Commander, U.S. Strategic Command, through the Chairman of the Joint Chiefs of Staff, shall:

5.6.1. Establish and maintain a Joint OPSEC Support Element to provide OPSEC training, program review, surveys, and plans and exercise support to the Combatant Commands.

5.6.2. Provide OPSEC management oversight for the Combatant Commanders.

5.7. The Director, National Security Agency, under the authority, direction, and control of the USD(I), in addition to the tasks in Reference (b), shall act as the Federal Executive Agent for interagency OPSEC training, and in that capacity shall maintain an IOSS to assist Executive Departments and Agencies, as needed, in establishing OPSEC programs, conducting OPSEC surveys, providing OPSEC services, and developing and providing interagency OPSEC training and awareness courses and products.

5.8. The Director, Defense Intelligence Agency, under the authority, direction, and control of the USD(I), shall provide intelligence and counterintelligence threat analysis to support OPSEC planning to all DoD Components that submit validated production requirements.

5.9. The Director, Defense Security Service, under the authority, direction and control of the USD(I), shall:

5.9.1. Comply 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.

5.9.2. Request assistance, as necessary, from the applicable Heads of the DoD Components to conduct inspections required by subparagraph 5.9.1., above.

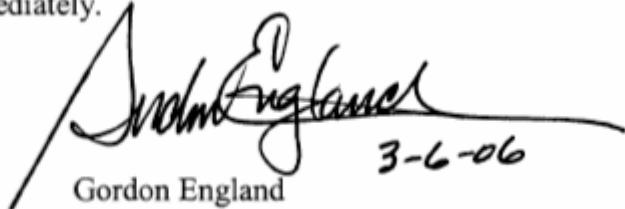
5.9.3. When requested, coordinate with and assist user Agencies in OPSEC surveys for contractors performing classified contracts and participating in the NISP.

6. INFORMATION REQUIREMENTS

The reporting requirements in this Directive have been assigned Report Control Symbol (RCS) DD-INTEL(A)2228 in accordance with DoD 8910.1-M (Reference (f)).

7. EFFECTIVE DATE

This Directive is effective immediately.



A handwritten signature in black ink, appearing to read "Gordon England". To the right of the signature is the date "3-6-06". Below the signature, the name "Gordon England" is printed in a smaller, sans-serif font.

Enclosures – 2

- E1. References, continued
- E2. Definitions

E1. ENCLOSURE 1

REFERENCES, continued

- (e) DoD Directive 5230.9, "Clearance of DoD Information for Public Release," April 9, 1996
- (f) DoD 8910.1-M, "DoD Procedures for Management of Information Requirements," June 30, 1998

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Acquisition Program. A directed, funded effort that provides a new, improved, or continuing material, weapon, or information system or service capability in response to an approved need.

E2.1.2. Information Operations (IO). The integrated employment of the core capabilities of Electronic Warfare, Computer Network Operations, Psychological Operations, Military Deception, and Operations Security, together with specified support and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making while protecting our own.

E2.1.3. Operations Security (OPSEC). A process of identifying critical information and analyzing friendly actions attendant to military operations and other activities including:

E2.1.3.1. Identify those actions that can be observed by adversary intelligence systems.

E2.1.3.2. Determining indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical intelligence in time to be useful to adversaries.

E2.1.3.3. Selecting and executing measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

E2.1.4. OPSEC Assessment. An evaluative process, usually conducted annually, of an operation, activity, exercise, or support function to determine the likelihood that critical information can be protected from the adversary's intelligence.

E2.1.5. OPSEC Coordinator. An individual fully trained in OPSEC located at a subordinate level, who works in coordination with the OPSEC Program Manager.

E2.1.6. OPSEC Indicators. Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information.

E2.1.7. OPSEC Program Manager. A dedicated, full-time OPSEC professional assigned to develop and manage the commands'/units' OPSEC program.

E2.1.8. OPSEC Program. A comprehensive process incorporating the principles and practices of OPSEC into an organization.

E2.1.9. OPSEC Survey. Conducted at least once every three years, a survey is a collection effort by a team of subject matter experts to reproduce the intelligence image projected by a specific operation or function simulating hostile intelligence processes.