Department of Defense
DIRECTIVE

NUMBER 5205.02E
June 20, 2012

USD(I)

SUBJECT: DoD Operations Security (OPSEC) Program

References: See Enclosure 1

1. PURPOSE. This Directive:

a. Reissues DoD Directive (DoDD) 5205.02 (Reference (a)) to update established policy and assigned responsibilities governing the DoD OPSEC program, and incorporate the requirements of National Security Decision Directive Number 298 (Reference (b)) that apply to the DoD.

b. Pursuant to Reference (b), establishes the Director, National Security Agency (DIRNSA) as the Federal Executive Agent (EA) for interagency OPSEC training and assigns responsibility for maintaining an Interagency OPSEC Support Staff (IOSS).

2. APPLICABILITY. This Directive applies to the OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint 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 within the DoD (hereinafter referred to collectively as the "DoD Components").

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that all DoD missions, functions, programs, and activities shall be protected by an OPSEC program that implements DoD Manual 5205.02 (Reference (c)).

a. OPSEC shall be considered across the entire spectrum of DoD missions, functions, programs, and activities. The level of OPSEC to apply is dependent on the threat, vulnerability, and risk to the assigned mission, function, program, or activity, and available resources.

b. OPSEC and other security and information operations programs shall be closely coordinated to account for force protection and the security of information and activities.

c. DoD personnel shall maintain essential secrecy of information that is useful to adversaries and potential adversaries to plan, prepare, and conduct military and other operations against the United States and shall safeguard such information from unauthorized access and disclosure in accordance with DoD Manual 5200.01 (Reference (d)).

d. The OPSEC process shall be used to identify and mitigate indicators of U.S. intentions, capabilities, operations, and activities.

e. OPSEC countermeasures shall be employed to deny to adversaries and potential adversaries indicators that reveal critical information about DoD missions and functions.

5. RESPONSIBILITIES. See Enclosure 2.

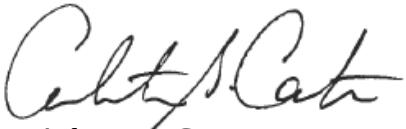
6. INFORMATION COLLECTION REQUIREMENTS. The reporting requirements in this Directive have been assigned Report Control Symbol DD-INTEL(A)2228 in accordance with DoD 8910.01-M (Reference (e)).

7. RELEASABILITY. UNLIMITED. This Directive is approved for public release and is available on the Internet from the DoD issuances website at http://www.dtic.mil/whs/directives.

8. EFFECTIVE DATE

a. This Directive is effective June 20, 2012.

b. This Directive must be reissued, cancelled, or certified current within 5 years of its publication in accordance with DoD Instruction 5025.01 (Reference (f)). If not, this Directive will expire effective June 20, 2022 and be removed from the DoD Issuances Website.



Ashton B. Carter
Deputy Secretary of Defense

Enclosures
1. References
2. Responsibilities

Glossary

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5205.02, "DoD Operations Security (OPSEC) Program," March 6, 2006 (hereby cancelled)
(b) National Security Decision Directive Number 298, "National Operations Security Program," January 22, 1988
(c) DoD 5205.02-M, "DoD Operations Security (OPSEC) Program Manual," November 3, 2008
(d) DoD Manual 5200.01, "DoD Information Security Program," February 24, 2012
(e) DoD 8910.1-M, "Department of Defense Procedures for Management of Information Requirements," June 30, 1998
(f) DoD Instruction 5025.01, "DoD Directives Program," October 28, 2007
(g) Deputy Secretary of Defense Memorandum, "Reserve Component Joint Web Risk Assessment Cell," February 12, 1999
(h) DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)," February 28, 2006
(i) Secretary of Defense Memorandum, "Strategic Communication and Information Operations in the DoD," January 25, 2011
(j) DoD Instruction 5200.39, "Critical Program Information (CPI) Protection Within the Department of Defense," July 16, 2008
(k) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," current edition
(l) Chairman of the Joint Chiefs of Staff Instruction 3213.01C, "Joint Operations Security," July 17, 2008

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I), in addition to the responsibilities in section 11 of this enclosure, shall:

a. Establish and oversee the implementation of policies and procedures for the conduct of DoD OPSEC.

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

c. Coordinate and synchronize OPSEC matters and policies affecting more than one DoD Component and other Federal agencies.

e. Develop guidance for conducting OPSEC assessments and surveys.

f. In coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), develop standards and procedures for the evaluation and protection, when necessary, of unclassified and classified contract efforts.

g. Assign DoD representatives to the IOSS.

h. In coordination with the Under Secretary of Defense for Policy (USD(P)), the Under Secretary of Defense for Personnel and Readiness (USD(P&R)), and the CJCS, oversee the establishment and maintenance of a professionally trained and educated OPSEC workforce as part of information operations (IO) force development.

i. In accordance with Deputy Secretary of Defense Memorandum (Reference (g)), develop procedures and guidelines to be implemented by the DoD Components for OPSEC reviews of DoD information shared via Internet-based capabilities.

j. Establish a training consortium comprised of subject matter experts from the OPSEC community to identify training requirements; review and update OPSEC curriculum; and recommend solutions to recognized training issues.

2. DIRNSA. The DIRNSA, under the authority, direction, and control of the USD(I), in addition to the tasks in Reference (b) and responsibilities in section 11 of this enclosure shall act as the Federal Executive Agent for interagency OPSEC training, 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.

3. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). The Director, DIA, under the authority, direction, and control of the USD(I), in addition to the responsibilities in section 11 of this enclosure, shall provide intelligence and counterintelligence threat analysis to support OPSEC planning to all DoD Components.

4. DIRECTOR, DEFENSE SECURITY SERVICE (DSS). The Director, DSS, under the authority, direction, and control of the USD(I), in addition to the responsibilities in section 11 of this enclosure, shall:

a. Verify compliance with OPSEC requirements incorporated in classified contracts during scheduled security reviews performed under the National Industrial Security Program (NISP) in accordance with DoD 5220.22-M (Reference (h)). If required, prescribe OPSEC countermeasures against specific threats for the protection of critical and sensitive information. On U.S. Government controlled installations, such inspections shall be performed only when the contractor location is a separately cleared facility under the NISP and the installation commander requests the security inspection.

b. In coordination with DoD Components, as necessary, conduct inspections when required. When requested, coordinate with and assist user agencies in OPSEC surveys of contractors performing classified contracts and participating in the NISP.

5. USD(P). The USD(P), in addition to the responsibilities in section 11 of this enclosure, shall:

a. As the Principal Staff Assistant for IO, serve as the principal policy development, oversight, and coordinating authority for the integration of OPSEC as a warfighting enabler, in accordance with Secretary of Defense Memorandum (Reference (i)).

b. Review Combatant Commander operations and plans for OPSEC integration.

c. In coordination with the USD(I), USD(P&R), and CJCS, oversee the establishment and maintenance of a professionally trained and educated OPSEC workforce as part of IO force development.

6. USD(AT&L). The USD(AT&L), in addition to the responsibilities in section 11 of this enclosure, shall:

a. Ensure an OPSEC plan is included as a countermeasure in program protection plans for research, development, and acquisition programs when critical program information has been identified by the program manager in accordance with DoD Instruction 5200.39 (Reference (j)).

b. In coordination with the USD(I), develop standards and procedures for the evaluation and protection, when necessary, of unclassified and classified contract efforts.

7. USD(P&R). The USD(P&R), in addition to the responsibilities in section 11 of this enclosure, shall, in coordination with the USD(I), USD(P), and CJCS, oversee the establishment and maintenance of a professionally trained and educated OPSEC force as part of IO force development.

8. ASSISTANT SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS (ASD(PA)). The ASD(PA), in addition to the responsibilities in section 11 of this enclosure, shall:

a. Develop policy and guidance to ensure OPSEC is incorporated into the public affairs release of information process.

b. Coordinate with the USD(I) and DIRNSA/CHCSS to ensure specialized OPSEC training is included in the curriculum for public affairs specialists and officers at the beginner and advanced levels of training at the Defense Information School.

9. DoD CHIEF INFORMATION OFFICER (DoD CIO). The DoD CIO, in addition to the responsibilities in section 11 of this enclosure, shall address OPSEC and classification through compilation of data when developing policies and initiatives regarding information sharing capabilities that are accessible across the enterprise and shall also develop procedures to mitigate risks.

10. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA). In accordance with Reference (g), the Director, DISA, under the authority, direction, and control of the DoD CIO and in addition to the responsibilities in section 11 of this enclosure, shall conduct ongoing OPSEC assessments of Combatant Command, OSD, Defense Agency, and DoD Field Activity websites.

11. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall establish OPSEC programs with full-time OPSEC program managers and coordinators at appropriate command levels to promote an understanding and practice of OPSEC among all personnel. The Heads of the DoD Components shall direct that:

a. OPSEC responsibilities are assigned by commanders and directors to the functional area of their choice.

b. Guidance is established for identifying and updating critical information as missions change.

c. A process is in place to report to appropriate channels within the Component disclosures of critical information so that mitigating actions can be implemented.

d. Dedicated manpower, funding, and resources are available to implement the OPSEC program. DoD Components will account and plan for resources in accordance with the Planning, Programming, Budgeting, and Execution System.

e. Annual OPSEC assessments are conducted. An OPSEC assessment may include program reviews, Inspector General inspections, or higher headquarters assessments that specifically address OPSEC.

f. An annual review and validation of Component OPSEC programs is submitted to the USD(I).

g. Threat-based comprehensive OPSEC surveys are conducted, at a minimum, every 3 years. Available automated risk analysis tools that facilitate the OPSEC process should be leveraged to aid in the identification of vulnerabilities and applicable countermeasures.

(1) Activities that warrant OPSEC surveys include but are not limited to research, development, test and evaluation; acquisitions; treaty verification; nonproliferation protocols; international agreements; force protection operations; special access programs; and activities that prepare, sustain, or employ Military Services over the range of military operations.

(2) DoD Components shall identify and prioritize OPSEC survey requirements and outline procedures for requesting OPSEC survey support from the appropriate organizations.

h. OPSEC support capabilities are utilized for program development and review, planning, training, surveys, assessments, and related support, as required.

i. OPSEC is coordinated and integrated with other U.S. Government agencies, allies, and coalition partner programs, operations, and activities as appropriate.

j. In accordance with Reference (c), policies and procedures are established for the review of unclassified information for OPSEC considerations and data aggregation prior to public release.

k. The risk of exposure to critical or classified information (alone or through compilation) is mitigated by providing OPSEC awareness training and guidance to the Component for those using DoD Internet services, other Internet-based capabilities, emerging technologies, or developing information sharing environments that are accessible across the enterprise.

l. OPSEC program managers, coordinators, IO professionals, public affairs personnel, contracting specialists, and personnel responsible for the review and approval of information intended for public release have received specialized OPSEC training for their duties in accordance with Reference (c). The general workforce shall receive OPSEC awareness training upon initial entry to duty (to include entry to accession programs such as basic training, commissioning sources, and internships) and annually thereafter.

m. Guidance is issued to ensure that DoD unclassified and classified contract requirements properly reflect OPSEC responsibilities and that those responsibilities are included in contracts

when applicable. For classified contracts specifically, in accordance with paragraph 4.a. and 4.b. of this enclosure, and in coordination with the Director, DSS, ensure adequacy of industrial security efforts for OPSEC countermeasures outlined in classified contracts that fall under the NISP.

12. SECRETARIES OF THE MILITARY DEPARTMENTS. The Secretaries of the Military Departments, in addition to the responsibilities in section 11 of this enclosure, shall:

a. Establish an OPSEC capability that provides for program development, planning, training, assessments, surveys, and operational support as required.

b. Require deploying personnel to complete OPSEC training specific to the operating area.

c. Direct the establishment of OPSEC working groups at military installations to advise and support installation operations, threat, and force protection working groups.

d. In coordination with the Director, DISA, establish and maintain a capability to conduct ongoing OPSEC assessments of component websites.

13. CJCS. The CJCS, in addition to the responsibilities in section 11 of this enclosure, shall:

a. As the joint proponent for OPSEC, oversee contingency planning and operational integration of OPSEC across the Combatant Commands.

b. Evaluate and oversee joint OPSEC training to ensure Combatant Command requirements are met satisfactorily within the joint training system and meet the requirements of a professionally trained and educated OPSEC workforce as part of IO force development.

c. Establish and maintain a joint OPSEC support element to provide OPSEC training, program development and reviews, surveys, assessments, and plans and exercise support to the Combatant Commands.

d. Coordinate with the USD(I), USD(P), and USD(P&R) for the establishment and maintenance of a professionally trained and educated force as part of IO force development.

14. COMMANDERS OF THE COMBATANT COMMANDS. The Commanders of Combatant Commands, in addition to the responsibilities in section 11 of this enclosure, shall integrate OPSEC into all contingency planning and operations and notify the CJCS of OPSEC requirements.

15. COMMANDERS OF THE GEOGRAPHIC COMBATANT COMMANDS. The Commanders of the geographic Combatant Commands, in addition to the responsibilities in

sections 11 and 14 of this enclosure, shall develop area specific OPSEC training for deploying Service members to complete prior to arrival in theater.

16. COMMANDER UNITED STATES SPECIAL OPERATIONS COMMAND (USSOCOM). The Commander, USSOCOM, in addition to the responsibilities in sections 11 and 14 of this enclosure, shall:

a. Establish and maintain an OPSEC support element to provide the command and its subordinates with program development, planning, training, assessment, survey, and readiness training tailored to the unique special operations mission.

b. As a force provider for special operations forces, liaise with geographic Combatant Commanders and the joint OPSEC support element to ensure preparedness of theater special operations commands.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASD(PA)	Assistant Secretary of Defense for Public Affairs
CJCS	Chairman of the Joint Chiefs of Staff
DIA	Defense Intelligence Agency
DIRNSA	Director, National Security Agency
DoD CIO	DoD Chief Information Officer
DoDD	DoD Directive
DSS	Defense Security Service
EA	Executive Agent
IO	information operations
IOSS	Interagency OPSEC Support Staff
NISP	National Industrial Security Program
OPSEC	operations security
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USSOCOM	United States Special Operations Command

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purposes of this Directive.

adversary intelligence systems. Resources and methods available to and used by an adversary for the collection and exploitation of critical information or indicators thereof. This term and its definition are approved for inclusion in the next edition of Joint Publication 1-02 (Reference (k)).

countermeasure. Defined in Reference (c).

critical information. Defined in Reference (k).

essential secrecy. Defined in Chairman of the Joint Chiefs of Staff Instruction 3213.01C (Reference (l)).

exploitation. The process of obtaining information from any source and taking advantage of it.

friendly actions. An operation or activity that is carried out by a country, organization, or individual that is allied to the U.S. military.

indicator. Defined in Reference (c).

OPSEC. A process of identifying critical information and analyzing friendly actions attendant to military operations and other activities to: identify those actions that can be observed by adversary intelligence systems; determine indicators and vulnerabilities that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and determine which of these represent an unacceptable risk; then select and execute countermeasures that eliminate the risk to friendly actions and operations or reduce it to an acceptable level.

OPSEC assessment. An evaluative process of an organization, operation, activity, exercise, or support function to determine if sufficient countermeasures are in place to protect critical information. This term and its definition are approved for inclusion in the next edition of Reference (k).

OPSEC coordinator. An individual trained in OPSEC located at a subordinate level, who works in coordination with the OPSEC program manager or primary representative.

OPSEC planner. A functional expert trained and qualified to plan and execute OPSEC.

OPSEC process. Defined in Reference (c).

OPSEC program manager. A full-time appointee or primary representative assigned to develop and manage an OPSEC program.

OPSEC survey. An application of the OPSEC process by a team of subject matter experts to conduct a detailed analysis of activities associated with a specific organization, operation, activity, exercise, or support function by employing the known collection capabilities of potential adversaries. This term and its definition are approved for inclusion in the next edition of Reference (k).