Department of Defense

DIRECTIVE

NUMBER 5205.~~02~~02E

~~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, 1988[1]~~

~~(c) DoD Directive S-3600.1, "Information Operations (IO) (U)," December 9, 1996[2]~~

~~(d) Joint Publication 1-02, "DoD Dictionary of Military and Associated Terms," April 12, 2001~~

~~(e) through (f), see~~ See Enclosure 1

1. ~~REISSUANCE AND~~ PURPOSE

. This Directive:

~~1.1~~a. Reissues DoD Directive (DoDD) 5205.02 (Reference (a~~)~~)) to update established policy and assigned responsibilities governing the DoD ~~Operations Security (~~OPSEC~~) Program~~ program, and ~~incorporates~~incorporate the requirements of National Security Decision Directive Number 298 (Reference (b~~)~~)) that apply to the ~~Department of Defense~~DoD.

~~1.2. Under~~ b. Pursuant to Reference (b), ~~designates~~establishes the Director, National Security Agency (DIRNSA) as the Federal Executive Agent (EA) for interagency OPSEC training~~.~~

~~1.3. Underscores the importance of~~ and assigns responsibility for maintaining an Interagency 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)).~~Support Staff (IOSS).

~~[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 applies to the Office of the Secretary of DefenseOSD, 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 inwithin the Department of Defense (hereafterDoD (hereinafter 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. See Glossary.

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

~~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~~

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 ~~ensure that all aspects of sensitive operations and~~ account for force protection ~~are protected~~and the security of information and activities.

~~4.3. The~~ c. DoD personnel shall maintain essential secrecy of information ~~critical~~that is useful to adversaries ~~in their planning, preparing and conducting~~ and potential adversaries to plan, prepare, and conduct military and other operations against the United States and shall ~~be maintained.~~

~~4.3.1. Adversary intelligence collection threats include the exploitation of publicly available information often obtained through open networks and~~ safeguard such 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.~~from unauthorized access and disclosure in accordance with DoD Manual 5200.01 (Reference (d)).

~~4.3.2~~ d. The OPSEC ~~analytic~~ process ~~is based on the identification~~shall be used to identify and ~~mitigation of these~~ mitigate indicators of U.S. intentions, capabilities, operations, and activities.

~~4.3.3~~ e. OPSEC ~~measures~~countermeasures shall be employed to deny ~~indicators~~ to adversaries and potential adversaries indicators 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. See Enclosure 2.

~~5.1. The Under~~

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 upon its publication to the DoD issuances website.

b. This Directive must be reissued, cancelled, or certified current within 5 years of its publication in accordance with DoDI 5025.01 (Reference (s)). If not, this Instruction will expire effective 10 YEARS FROM PUBLICATION DATE and be removed from the DoD Issuances Website.

Ashton B. Carter
Deputy Secretary of Defense ~~for Intelligence (USD(I)) shall:~~

~~5.~~Enclosures
1. References
2. Responsibilities
Glossary

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5205.02, "DoD Operations Security 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) Deputy Secretary of Defense Memorandum, "Reserve Component Joint Web Risk Assessment Cell," February 12, 1999
(g) DoD 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006
(h) Secretary of Defense Memorandum, "Strategic Communication and Information Operations in the DoD," January 25, 2011
(i) DoD Instruction 5200.39, "Critical Program Information (CPI) Protection Within the Department of Defense," July 16, 2008
(j) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," current edition
(k) 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 ~~the DoD OPSEC Program, including monitoring, evaluating, and periodically reviewing all DoD OPSEC activities~~DoD OPSEC.

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

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

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

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

~~5.1.6~~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.

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

~~5.2. The~~ h. In coordination with 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~~ (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 ~~and contingency plans to ensure OPSEC integration~~(IO) force development.

~~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~~

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

j. Establish ~~an OPSEC program focused on command involvement, assessments, surveys,~~ a 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,~~ consortium comprised of subject matter experts from the OPSEC community to identify training~~, assessment, surveys, and readiness~~ requirements; review and update OPSEC curriculum; and recommend solutions to recognized training issues.

~~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~~

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, ~~and in that capacity shall~~ maintain an IOSS to assist ~~Executive Departments~~executive departments and ~~Agencies~~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.~~

3. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). The Director, ~~Defense Intelligence Agency~~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 ~~that submit validated production requirements.~~ .

~~5.9.~~

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

~~5.9.1. Comply~~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 (g)). If required, ~~ensure that the~~ prescribe OPSEC countermeasures against specific threats ~~and OPSEC measures are identified that shall protect the~~for the protection of critical ~~or~~and sensitive information. On ~~military~~U.S. Government controlled installations, such inspections shall be performed only when ~~requested by~~the contractor location is a separately cleared facility under the NISP and the installation commander requests the security inspection.

~~5.9.2. Request assistance~~b. In coordination with DoD Components, as necessary, ~~from the applicable Heads of the DoD Components to~~ conduct inspections when required ~~by subparagraph 5.9.1., above.~~

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

~~6. INFORMATION REQUIREMENTS~~

5. USD(P). The ~~reporting requirements~~ USD(P), in addition to the responsibilities in section 11 of this ~~Directive have been assigned Report Control Symbol (RCS) DD-INTEL(A)2228~~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 (h)).

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 ~~8910.1-M~~Instruction 5200.39 (Reference (~~f~~i)).

~~7. EFFECTIVE DATE~~

This Directive is effective immediately.

3-6-06

Gordon England

~~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~~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 (f), 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 ~~(OPSEC).~~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 (j)).

countermeasure. Defined in Reference (c).

critical information. Defined in Reference (j).

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

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 including:

E2.1.3.1. Identifyto: identify those actions that can be observed by adversary intelligence systems.

E2.1.3.2. Determining; determine indicators and vulnerabilities that hostileadversary intelligence systems might obtain that could be interpreted or pieced together to derive critical intelligenceinformation 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.

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 Assessmentassessment. An evaluative process, usually conducted annually, of an organization, operation, activity, exercise, or support function to determine the likelihood thatif sufficient countermeasures are in place to protect critical information can be protected from the adversary's intelligence.. This term and its definition are approved for inclusion in the next edition of Reference (j).

E2.1.5. OPSEC Coordinatorcoordinator. An individual fully trained in OPSEC located at a subordinate level, who works in coordination with the OPSEC Program Manager.program manager or primary representative.

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

OPSEC professionalprocess. Defined in Reference (c).

OPSEC program manager. A full-time appointee or primary representative assigned to develop and manage the commands'/units'an 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. An application of the OPSEC ~~Survey. Conducted at least once every three years, a survey is a collection effort~~process by a team of subject matter experts to ~~reproduce the intelligence image projected by~~conduct a detailed analysis of activities associated with a specific organization, operation, activity, exercise, or support function ~~simulating hostile intelligence processes.~~by employing the known collection capabilities of potential adversaries. This term and its definition are approved for inclusion in the next edition of Reference (j).