Department of Defense
MANUAL

NUMBER 5205.02-M
November 3, 2008

USD(I)

SUBJECT: DoD Operations Security (OPSEC) Program Manual

References: See Enclosure 1

1. PURPOSE. In accordance with the authority in DoD Directive (DoDD) 5205.02 (Reference (a)), this Manual implements policy, assigns responsibilities, and provides procedures for managing DoD OPSEC programs.

2. APPLICABILITY. This Manual applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff 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 Department of Defense (hereafter referred to collectively as the "DoD Components").

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy according to Reference (a) to establish and maintain OPSEC programs to ensure national security-related missions and functions are protected. This Manual lists baseline requirements. Nothing in this Manual abrogates or limits the authority of the Heads of DoD Components to apply more stringent OPSEC standards as commanders and/or directors deem necessary.

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. Procedures for managing OPSEC programs are outlined in Enclosures 3 through 7.

7. INFORMATION REQUIREMENTS. The annual reporting requirements described in Enclosure 2, paragraph 4.a.(10), have been assigned Report Control Symbol (RCS) DD-INTEL(A)2228 in accordance with DoD 8910.1-M (Reference (c)).

8. RELEASEABILITY. UNLIMITED. This Manual is approved for public release. Copies may be obtained through the Internet from the DoD Issuances Web Site at http://www.dtic.mil/whs/directives.

9. EFFECTIVE DATE. This Manual is effective immediately.

James R. Clapper, Jr.
Under Secretary of Defense for Intelligence

Enclosures
1. References
2. Responsibilities
3. Program Management
4. OPSEC Assessments and Surveys
5. Information Protection Requirements
6. Contract Requirements
7. OPSEC Education, Training and Awareness

Glossary

TABLE OF CONTENTS

REFERENCES 5

RESPONSIBILITIES 6

UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)) 6
DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA) 6
DIRECTOR, DEFENSE SECURITY SERVICE (DSS) 6
DIRECTOR, NATIONAL SECURITY AGENCY (DIRNSA) 6
UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)) 6
HEADS OF THE DoD COMPONENTS 7
CHAIRMAN OF THE JOINT CHIEFS OF STAFF AND COMBATANT COMMANDERS 8
COMMANDER, UNITED STATES STRATEGIC COMMAND (USSTRATCOM) 8

PROGRAM MANAGEMENT 9

INTRODUCTION 9
DoD COMPONENT OPSEC PROGRAM MANAGER 9
SUBCOMPONENT OPSEC PROGRAM LEVELS 9

OPSEC PROCESS 12
PROGRAM REVIEW CHECKLIST 15

OPSEC ASSESSMENTS AND SURVEYS 17

OPSEC ASSESSMENTS 17
OPSEC SURVEYS 18
ASSESSMENT AND SURVEY COMPARISON 19

ANALYSIS RATINGS CRITERIA 21

INFORMATION PROTECTION REQUIREMENTS 27

CONTENT REVIEWS 30
INFORMATION SYSTEMS 31
HANDLING REQUIREMENTS 31

CONTRACT REQUIREMENTS 32

INTRODUCTION 32
PROCEDURES 32

OPSEC EDUCATION, TRAINING AND AWARENESS 34

INTRODUCTION 34
EDUCATION AND TRAINING 34
AWARENESS TRAINING 35

GLOSSARY 36

ABBREVIATIONS AND ACRONYMS 36
DEFINITIONS 36

TABLES

1. OPSEC Program Review Checklist 15
2. OPSEC Assessment and Survey Comparison 20
3. Critical Information Value Matrix 21
4. Threat Value Matrix 24
5. Vulnerability Values 27
6. Probability of Critical Information Loss 27
7. Risk Assessment 28
8. Risk Assessment Process Example 28

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5205.02, "DoD Operations Security (OPSEC) Program," March 6, 2006
(b) National Security Decision Directive No. 298, "National Operations Security Program," January 22, 1988
(c) DoD 8910.1-M, "DoD Procedures for Management of Information Requirements," June 30, 1998
(d) DoD Directive 3020.40, "Defense Critical Infrastructure Program (DCIP)," August 19, 2005
(e) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008
(f) DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 6, 1999
(g) Deputy Secretary of Defense Memorandum, "DoD Web Site Administration Policies and Procedures," November 25, 1998, as amended[1]
(h) DoD Regulation 5200.1-R, "Information Security Program," January 14, 1997
(i) DoD Regulation 5220.22-R, "Industrial Security Regulation," December 4, 1985
(j) DoD Instruction 3608.12, "Joint Information Operations (IO) Education," November 4, 2005
(k) Joint Publication 1-02, "DoD Dictionary of Military and Associated Terms," as amended
(l) Section 552a of title 5, United States Code

[1] Copies may be obtained from the Internet at http://www.defenselink.mil/webmasters/

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I) shall:

a. Establish and oversee the DoD OPSEC Program and provide policies and procedures for DoD Component implementation of the program, including monitoring, evaluating, and periodically reviewing all DoD Component OPSEC programs.

b. Provide reporting guidance to the Heads of the DoD Components prior to the end of each fiscal year.

c. Compile and analyze DoD Component reports, and report annually to the Secretary of Defense on the status of the DoD OPSEC Program.

2. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). The Director, DIA, shall carry out responsibilities set forth in Reference (a).

3. DIRECTOR, DEFENSE SECURITY SERVICE (DSS). The Director, DSS, shall carry out responsibilities set forth in Reference (a).

4. DIRECTOR, NATIONAL SECURITY AGENCY (DIRNSA). The DIRNSA, under the authority, direction, and control of the USD(I), shall act as the Federal Executive Agent for the Interagency OPSEC Support Staff (IOSS) in accordance with Reference (a) and National Security Decision Directive No. 298 (Reference (b)). The IOSS shall:

a. Support the DoD Components in establishing OPSEC programs and conducting OPSEC surveys and assessments.

b. Provide OPSEC education and awareness training to employees and supporting contractors designated by the Heads of the DoD Components.

c. Report annually to the USD(I) on the state of the IOSS.

5. UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)). The USD(P) shall:

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

b. Review all combatant commander operations and contingency plans to ensure OPSEC integration.

6. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall:

a. Implement the procedures prescribed in this Manual and ensure that supplemental guidance and procedures are in accordance with Reference (a) and this Manual.

(1) Integrate OPSEC in all activities and operations that prepare, sustain, or employ U.S. Armed Forces during war, crisis, or peace including, but not limited to, research, development, test, and evaluation; special access programs; DoD contracting; treaty verification; nonproliferation protocols; international agreements; force protection; and release of information to the public.

(2) Maintain an OPSEC program managed by a full-time program manager at the senior level who shall be responsible for the direction and administration of the program consistent with Enclosure 3.

(3) Identify critical information and develop policies and procedures for its protection.

(4) Plan, program, and budget for implementing and maintaining OPSEC programs.

(5) Determine OPSEC assessment and survey requirements for activities within their Components, establish guidance for conducting assessments and surveys, and supplement the provisions of this Manual to meet specific needs consistent with Enclosure 4.

(6) Ensure that compliance with policy for content reviews of information intended for release outside the control of the organization, including release to the public, is appropriately evaluated during program reviews and other oversight activities consistent with Enclosure 5. Evaluation shall include assessment of the quality and effectiveness of integrating OPSEC into the organization's policies and procedures to identify and protect critical information.

(7) Ensure guidance is established that requires OPSEC planning be integrated into the planning, development, and implementation stages of net-centric programs and operating environments, and that data aggregation concerns are assessed and risk-management strategies applied consistent with Enclosure 5.

(8) Ensure the integration of OPSEC requirements in classified and unclassified contracts consistent with Enclosure 6.

(9) Ensure OPSEC programs are reviewed annually and evaluated during inspections and other oversight activities at all levels of command. Annual reviews should assess if adequate resources are on hand to establish and maintain a successful program, if OPSEC Support Elements are being utilized and how effective they are, and if education, training, and awareness is being conducted throughout the workforce.

(10) Report to the USD(I) annually on the status of their Component OPSEC programs covering the previous fiscal year.

(11) Ensure establishment, execution, and evaluation of OPSEC awareness, education, and training programs consistent with Enclosure 7.

(12) Integrate OPSEC into critical infrastructure protection (CIP) planning in accordance with DoDD 3020.40 (Reference (d)) and this Manual.

(13) Coordinate and integrate OPSEC with other core Information Operations (IO) capabilities as applicable.

(14) Identify OPSEC requirements and coordinate with the USD(P) when establishing international cooperation agreements.

7. CHAIRMAN OF THE JOINT CHIEFS OF STAFF AND COMMANDERS OF COMBATANT COMMANDS. The Chairman of the Joint Chiefs of Staff and Commanders of Combatant Commands, in addition to the responsibilities in section 6, shall carry out responsibilities set forth in Reference (a).

8. COMMANDER, UNITED STATES STRATEGIC COMMAND (USSTRATCOM). The commander USSTRATCOM, through the Chairman of the Joint Chiefs of Staff shall:

a. Maintain the Joint OPSEC Support Element.

b. Coordinate with the USD(P) and support the Combatant Commands in planning and integrating joint OPSEC into their operations, to include:

(1) Planning for and executing OPSEC measures in support of assigned missions across the range of military operations.

(2) Providing OPSEC guidance to subordinate commands and supporting their responsibilities for integrating OPSEC into all command operations and joint activities.

(3) Providing OPSEC guidance and identifying command-critical information to all supporting commands, subordinate commands, other agencies, and public affairs offices.

(4) Coordinating OPSEC measures and their execution with those activities that cross command boundaries, such as strategic command and control and counter-drug operations, with other commands and agencies.

ENCLOSURE 3

PROGRAM MANAGEMENT

1. INTRODUCTION. Each DoD Component shall maintain an OPSEC program, resourced and focused on the protection of critical information through the establishment of procedures and the conduct of education and training.

2. DoD COMPONENT OPSEC PROGRAM MANAGER

a. The DoD Component OPSEC program manager, designated according to paragraph 6.a.(2) of Enclosure 2, shall be responsible for the following:

(1) Developing, communicating, and ensuring implementation of standards, policies, and procedures that supplement this Manual and meet specific needs of the DoD Component.

(2) Identifying necessary resources for the effective implementation of Component OPSEC programs.

(3) Advising the Head of the DoD Component in determining the program levels required for subcomponents as outlined in section 3 of this enclosure and in identifying which subcomponents require additional full- or part-time program managers and coordinators.

(4) Conducting program reviews to evaluate and assess the effectiveness and efficiency of the OPSEC program. OPSEC programs should be reviewed at least annually.

(5) Identifying and protecting critical information related to the CIP with appropriate OPSEC measures and advising supporting contractors of information protection requirements. In fulfilling this responsibility, program managers shall:

(a) Work with CIP planners to identify and protect, through the use of OPSEC measures, critical information related to CIP plans and programs and to integrate CIP into OPSEC assessments and surveys as needed.

(b) Assist CIP planners in promoting information sharing while safeguarding information that could harm DoD operations or that could jeopardize information-sharing agreements among stakeholders.

b. The DoD Component OPSEC program manager shall participate in training and education reviews and shall work with the USD(I) and the IOSS in identifying DoD OPSEC requirements.

3. SUBCOMPONENT OPSEC PROGRAM LEVELS. The following levels of involvement are provided as guidance to commanders and directors. Commanders and directors shall determine

what level of program is required for their mission. Based on the sensitivity of the mission and attendant threats, commanders and directors shall implement one of the following program levels.

a. Level I. A Level I program is a baseline OPSEC program for which the commander has determined a minimal level of OPSEC management and resources are required. A Level I program may fall under the oversight of a Level II or Level III program.

(1) A program coordinator (as defined in Reference (a)) shall be appointed in writing via a local policy letter signed by the commander or director. The policy letter shall be distributed to managers and supervisors, periodically reviewed, and updated when necessary.

(2) The program coordinator shall:

(a) Maintain and update the critical information list (CIL) that has been approved by the commander or director. Assigned personnel shall be knowledgeable of the designated critical information and measures in place to protect it.

(b) When necessary, implement the OPSEC process to protect a specific mission or activity. (See Appendix 1 of this enclosure for the OPSEC process.)

(c) Conduct an annual program review of the program. (See Appendix 2 of this enclosure for the program review checklist.) Program managers may supplement the Program Review Checklist at Appendix 2 of this enclosure with additional DoD Component-specific requirements.

(d) Participate in the review process of information intended for public release.

(e) Ensure that initial and annual refresher training on OPSEC is administered to all employees and contractors identified by the DoD Component.

b. Level II. A Level II program is a midlevel OPSEC program that requires a moderate amount of program management and dedicated resources. A Level II program shall meet all the Level I requirements. In addition, it shall be headed by a program manager (defined in Reference (a)), who shall:

(1) Develop supplemental guidance to this Manual on how the OPSEC program will be administered locally. Guidance shall be signed by the commander or director and distributed accordingly to organizational personnel.

(2) Ensure that initial and annual refresher training on OPSEC is provided to all employees and identified contractors; coordinate training for Level I OPSEC coordinators.

c. Level III. A Level III program consists of a full-time managed and resourced OPSEC program. Due to the level of oversight it has for subordinate units and/or the sensitivity of the

mission, this program requires substantial effort. A Level III program shall meet all the Level I and Level II requirements. In addition, the full-time program manager shall:

(1) Ensure newly-assigned program managers are trained within 90 days of assignment.

(2) Ensure OPSEC is incorporated into local exercises when applicable.

(3) Maintain a budget and have resources available to effectively implement and sustain the program.

(4) Provide support and guidance to other OPSEC managers and coordinators for whom he or she has oversight.

Appendixes

1. OPSEC Process
2. Program Review Checklist

APPENDIX 1 TO ENCLOSURE 3

OPSEC PROCESS

1. PURPOSE. The OPSEC process is a systematic method used to identify, control, and protect critical information. This appendix presents the five elements of the OPSEC process as steps. These steps may or may not be used in sequential order but all elements must be present to conduct OPSEC analysis.

2. STEPS IN THE OPSEC PROCESS

a. Identify Critical Information. Critical information is information about DoD activities, intentions, capabilities, or limitations that an adversary seeks in order to gain a military, political, diplomatic, economic, or technological advantage. Such information, if revealed to an adversary, may prevent or degrade mission accomplishment, cause loss of life, or damage friendly resources.

(1) Critical information will vary based on the organization's role within the Department of Defense. Critical information in operational organizations is often easy to recognize, however in support or administratively focused organizations, critical information may be more difficult to identify. When going through the process of identifying critical information, be sure to consider all functional areas within the organization. The organization's administrative staff may have valuable information that should also be assessed for its criticality.

(2) Critical information is best identified by the individuals responsible for planning and executing the organization's mission. Using an adversarial approach and asking what information an adversary would want to know about the mission is a helpful method when trying to identify what information is critical. The questions an adversary may ask are called "essential elements of friendly information." The answers to those questions are the critical information.

(3) Critical information is information that the organization has determined is valuable to an adversary. If obtained, this information will either impact the success of the organization or improve the likelihood of an adversary meeting their goals. For example:

(a) Military operations: The adversary learns of the time and location of a planned attack. As a result, losing the element of surprise could lead to significant casualties.

(b) Acquisition: The adversary learns of a new missile in the development phase that cannot be detected by adversary capabilities. As a result, the adversary begins development of countermeasures to defeat the new technology.

(c) Administration: The adversary obtains information about force protection equipment being sent to a unit operating in theater. As a result, the adversary changes its tactics, techniques, and procedures to defeat the equipment.

(4) From the examples given above, there are many areas within an organization where elements of critical information can be obtained. Commanders and directors, administrative staff, operational personnel, even personnel not directly assigned to the organization may handle portions of the organization's critical information. Therefore, it is important to have personnel from each functional area involved in the process of identifying critical information.

(5) Once the critical information has been identified, it should be compiled into a CIL approved by the commander or director and disseminated so that organizational personnel know what information is critical and requires protection.

b. Conduct a Threat Analysis. Threat information is necessary to develop appropriate countermeasures. The threat analysis includes identifying potential adversaries and their associated capabilities and intentions to collect, analyze, and exploit critical information and indicators.

(1) When conducting a threat analysis, organizations should seek support from their security, intelligence, and counterintelligence experts.

(2) A thorough threat analysis will answer the following questions.

(a) Who is the adversary? What is the adversary's intent and capability?

(b) What are the adversary's goals?

(c) What tactics does the adversary use?

(d) What does the adversary already know about the unit's mission? What critical information has already been exposed and is known by the adversary?

c. Conduct a Vulnerability Analysis. An OPSEC vulnerability exists when the adversary is capable of collecting critical information or indicators, analyzing it, and then acting quickly enough to impact friendly objectives. Conducting exercises, red teaming, and analyzing operations can help identify vulnerabilities.

d. Conduct a Risk Assessment. The risk assessment is the process of evaluating the risks to information based on susceptibility to intelligence collection and the anticipated severity of loss. It involves assessing the adversary's ability to exploit vulnerabilities that would lead to the exposure of critical information and the potential impact it would have on the mission. Determining the level of risk is a key element of the OPSEC process and provides justification for the use of countermeasures. Once the amount of risk is determined, consider cost, time, and effort of implementing OPSEC countermeasures to mitigate risk. Factors to consider include:

(1) The benefit and the effect of the countermeasure on reducing risk to the mission.

(2) The cost of the proposed countermeasure compared with the cost associated with the impact if the adversary exploited the vulnerability.

(3) The possibility that the countermeasure could create an OPSEC indicator.

e. Apply OPSEC Countermeasures. Countermeasures are designed to prevent an adversary from detecting critical information, provide an alternative interpretation of critical information or indicators (deception), or deny the adversary's collection system. If the amount of risk is determined to be unacceptable, countermeasures are then implemented to mitigate risk or to establish an acceptable level. Countermeasures should be coordinated and integrated with other IO core capabilities if applicable.

(1) Given the examples presented earlier with regard to military operations, acquisition, and administration; adversary exploitation of information could have been prevented with simple no-cost countermeasures. Proper safeguarding, limiting distribution, and shredding information when no longer needed are just a few examples of easily applied countermeasures.

(2) There are many best practices for countermeasures throughout the Department of Defense. Organizations may consult with OPSEC practitioners, security specialist, information technology specialists, and organizations with similar missions. However, countermeasures should not be regarded as risk-avoidance measures to be pulled from a list and implemented. Prior to recommending countermeasures, commanders or directors must carefully consider cost and their potential to degrade mission accomplishment.

APPENDIX 2 TO ENCLOSURE 3

PROGRAM REVIEW CHECKLIST

1. PURPOSE. This appendix provides a checklist at Table 1 that program managers and coordinators shall use to assess compliance with Reference (a) and this Manual. Program managers and coordinators should use this checklist upon assignment to their duties and annually thereafter.

2. SUPPLEMENTING GUIDANCE. The DoD Components are encouraged to supplement this checklist with additional requirements stipulated in DoD Component policies.

Table 1. OPSEC Program Review Checklist

ALL PURPOSE CHECKLIST		PAGE 1 OF 2 PAGES		
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA Operations Security (OPSEC) Program Review Checklist		OPR	DATE	
NO.	ITEM (Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)	YES	NO	N/A
	PROGRAM MANAGEMENT			
1.	Has the organization appointed in writing an OPSEC program manager or coordinator at the appropriate level? (DoDD 5205.02, paragraph 5.3.1.1.; DoDM 5205.02, Enclosure 3.)			
2.	Is the organization OPSEC manager or coordinator someone who is familiar with the operational aspects of the activity including the supporting intelligence, counterintelligence, and security countermeasures? (DoDD 5205.02, paragraph 2.2.)			
3.	Has the OPSEC manager or coordinator completed the appropriate training? (DoDM 5205.02, Enclosure 7.)			
4.	Does the organization have an OPSEC support capability that provides for program development, training, assessments, surveys, and readiness training? (DoDD 5205.02, paragraph 5.3.1.2.)			
5.	Has the OPSEC manager or coordinator developed local OPSEC guidance (regulations or operating procedures) for use of the OPSEC analytic process? (DoDD 5205.02, paragraph 5.3.1.3.)			
6.	Has the OPSEC manager or coordinator conducted an annual review and validation of the organization's OPSEC program? (DoDD 5205.02, paragraph 5.3.1.4.; DoDM 5205.02, Enclosure 3.)			
7.	Does the OPSEC manager ensure OPSEC assessments and surveys are conducted? (DoDM 5205.02, Enclosure 4.)			
8.	Does the OPSEC manager or coordinator provide sufficient support for subordinate units he or she has oversight for? (DoDD 5205.02, paragraph 5.3.1.4.)			

Table 1. OPSEC Program Review Checklist, continued

ALL PURPOSE CHECKLIST		PAGE 2 OF 2 PAGES		
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA Operations Security (OPSEC) Program Review Checklist		OPR	DATE	
NO.	ITEM (Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)	YES	NO	N/A
	PROGRAM MANAGEMENT			
9.	Is the OPSEC manager or coordinator involved in the review process of information intended for public release? (DoDM 5205.02, Enclosure 5.)			
10.	Has the organization ensured that critical information is identified and updated as missions change? (DoDD 5205.02, paragraph 5.3.4.)			
11.	Has the OPSEC manager or coordinator established, implemented, and maintained effective OPSEC education activities to include initial orientation and continuing and refresher training for assigned members? (DoDD 5205.02, paragraph 5.3.5.; DoDM 5205.02, Enclosure 7.)			
12.	Does the organization ensure OPSEC is included in activities that prepare, sustain, or employ U.S. Armed Forces during war, crisis, or peace, including research, development, test and evaluation; special access programs; DoD contracting; treaty verification; nonproliferation protocols; international agreements; force protection; and release of information to the public, when applicable? (DoDD 5205.02, paragraph 2.3.)			
13.	Does the OPSEC manager work with CIP planners to identify critical information related to CIP? (DoDM 5205.02, Enclosure 3.)			
14.	Are assigned personnel aware of the organization's critical information? (DoDM 5205.02, Enclosure 3.)			
15.	Has the component supplemented DoDD 5205.02 and DoDM 5205.02 and issued procedures for:			
	a. Integrating OPSEC planning into the planning, development, and implementation stages of net-centric programs and operating environments? (DoDM 5205.02, Enclosure 2.)			
	b. Conducting OPSEC assessments and surveys? (DoDD 5205.02, paragraph 5.3.2.; DoDM 5205.02, Enclosure 4.)			
	c. Handling, safeguarding, and destroying critical information? (DoDM 5205.02, Enclosure 5.)			
	d. A formal review of content for critical information, sensitivity, sensitivity in the aggregate, determination of appropriate audience, and distribution and release controls when releasing information? (DoDD 5205.02, paragraph 5.3.3.; DoDM 5205.02, Enclosure 5.)			
	e. Ensuring contract requirements properly reflect OPSEC requirements when appropriate? (DoDD 5205.02, paragraph 5.3.6.; DoDM 5205.02, Enclosure 6.)			

ENCLOSURE 4

OPSEC ASSESSMENTS AND SURVEYS

1. OPSEC ASSESSMENTS

a. Introduction

(1) This enclosure provides procedures for conducting OPSEC assessments. An assessment is an overall evaluation of the organization's OPSEC posture and is conducted by an organization's internal assets. The DoD Components shall assess their missions annually to determine the threat to U.S. operations and the potential loss of critical information.

(2) An assessment may also be conducted:

(a) When there is a need for an evaluation based on the sensitivity of the operation or program.

(b) When there is evidence that an adversary is attempting to gain critical information.

(c) Prior to the development of an OPSEC program or OPSEC plan. The assessment can establish an OPSEC profile by showing indicators that present vulnerabilities for an adversary to exploit. This will allow the program to be developed with fact-based knowledge of threats and vulnerabilities that must be addressed.

b. Procedures

(1) Heads of the DoD Components may supplement this Manual and stipulate more detailed procedures for conducting OPSEC assessments.

(a) An OPSEC assessment is conducted to assess an operation, activity, or exercise. Based on procedures currently in place, the assessment should determine the likelihood that critical information can be protected from adversarial intelligence collection.

(b) The assessment process shall examine the actual practices and procedures employed at an activity to determine if critical information may be inadvertently disclosed through the performance of normal organizational functions. The primary purpose is to evaluate and improve organizational effectiveness and control vulnerabilities of friendly actions or information.

(c) Assessments shall be conducted on a non-attribution basis and not used as a punitive tool. Assessments typically will be planned and conducted by the organization responsible for the activity. The results of the assessment will be given to the commander or

director of the organization being assessed. Commanders and directors are encouraged to share lessons learned.

(d) A typical assessment team is comprised of representatives from the organization's internal assets and may include counterintelligence, security, administrative, operations, communications, or public affairs personnel, or personnel from other areas important to the activity being assessed.

(2) DoD Component guidance for conducting assessments shall include:

(a) Consideration for the scope and limitations of the assessment. Provisions shall be made for factors such as the subordinate commander's intent for the assessment, resources available, size of the activity being assessed, and time available to conduct the assessment.

(b) The requirement to utilize the five-step OPSEC process in accordance with Appendix 1 of Enclosure 3.

(c) Designated checklists, evaluation criteria, and procedures for a planning phase, assessment phase, and analysis phase.

(d) Required use of the analysis ratings criteria in the appendix to this enclosure when analyzing assessed information.

2. OPSEC SURVEYS

a. Introduction

(1) This section establishes procedures for conducting OPSEC surveys. Surveys involve analyzing the activities associated with specific operations or programs to determine if there is adequate protection of critical information from adversary intelligence exploitation during the planning, preparation, execution, and post-execution phases of an operation or program.

(2) The depth and breadth of a survey depends on the degree of threat, the importance of the mission, and the harm that an adversary could inflict.

b. Procedures

(1) The Heads of DoD Components may supplement this Manual and stipulate more detailed procedures for conducting OPSEC surveys.

(a) An OPSEC survey shall be conducted every 3 years or when required by the commander or director. A survey seeks to reproduce the intelligence image in light of the known collection capabilities of potential adversaries.

(b) Surveys may be resource- and time-intensive. The DoD Components shall determine which activities in their command require surveys and develop implementing guidance for conducting them.

(c) The survey shall require that a team of experts look at an activity from an adversarial perspective to determine if critical information may be disclosed through normal operations and functions, to identify vulnerabilities, and to propose countermeasures to mitigate them.

(d) At the commander or director's discretion, the survey may focus on human intelligence (HUMINT), signals intelligence (SIGINT), measurement and signature intelligence (MASINT), open-source intelligence (OSINT), and/or geospatial intelligence (GEOINT) collection capabilities. These may include telecommunications monitoring, radio frequency monitoring, network and computer systems assessment, and open-source collection. Survey team members shall use collection techniques of known adversaries. Commanders and directors are encouraged to use existing OPSEC support capabilities to conduct surveys, if available.

(2) DoD Component guidance for conducting OPSEC surveys shall include:

(a) Procedures for scheduling surveys through OPSEC support capabilities or designated DoD activities capable of providing OPSEC support.

(b) Procedures for a planning, preparation, execution, and post-execution phase.

(c) Clearly defined rules of engagement for collection activities.

(d) Required use of the analysis ratings criteria in the appendix to this enclosure when analyzing information.

3. ASSESSMENT AND SURVEY COMPARISON. Table 2 describes how assessments and surveys differ in complexity.

Table 2. Assessment and Survey Comparison

OPSEC ASSESSMENT	OPSEC SURVEY
Purpose: To determine the likelihood that critical information can be protected based on procedures currently in place.	Purpose: To reproduce adversary collection capabilities against an organization to determine if critical information may be disclosed through normal operations and functions, to identify vulnerabilities, and to propose countermeasures.
Scale: Small in scale. Focused on evaluating OPSEC program effectiveness.	Scale: Large in scale. Focused on analysis of risks associated with an operation or organization's mission.
Frequency: Annually.	Frequency: Every 3 years or when operations or commanders dictate.
Resources: Internal resources (e.g., security, public affairs, communications personnel) are used to conduct the assessment.	Resources: External resources (e.g., OPSEC Support Elements, COMSEC monitors, red teams) are used collectively to conduct the survey with or without the use of indigenous resources.
Design: Assessment should include a planning, execution, and analysis phase. Minimal planning is required to conduct an assessment. A briefing or executive summary may be used to present findings.	Design: Survey planning is extensive and should include a planning, preparation, execution, and post-execution phase. A comprehensive report is generated.

Appendix
Analysis Rating Criteria

APPENDIX TO ENCLOSURE 4

ANALYSIS RATINGS CRITERIA

1. INTRODUCTION. The OPSEC analysis methodology uses a five-step OPSEC process. The basic risk analysis process allows the OPSEC manager to plan an effective OPSEC risk management strategy by analyzing and organizing information within each step of the process. An effective analysis is derived from using a basic calculation formula to establish specific risk levels relative to vulnerabilities based on the impact of the loss of the information, the threat posed to the information, and the susceptibility of the information to collection. Follow the steps and Tables 3 through 7 to determine the level of risk. Table 8 gives an example of application of the five steps.

2. STEP 1 – CRITICAL INFORMATION VALUE. Step 1 establishes the value of critical information based on its importance to both adversary and friendly objectives, and establishes subsequent impact to the organization or mission if that information is lost. Based on the scale in Table 3, assign a value from high to low for each piece of critical information identified.

Table 3. Critical Information Value Matrix

US		HI	MED HI	MED	MED LOW	LOW
ADVERSARY		Loss of CI will have a SEVERE impact on our ability to accomplish the mission	Loss of CI will probably have a SERIOUS impact on our ability to accomplish the mission	Loss of CI will likely have an APPRECIABLE impact on our ability to accomplish the mission	Loss of CI will possibly have a MODERATE impact on our ability to accomplish the mission	Loss of CI could have a MINOR impact on our ability to accomplish the mission
HI	Of CRITICAL importance to an adversary and obtaining the information CONSIDERABLY contributes to meeting adversary objectives	HI	MED HI	MED HI	MED HI	MED HI

Table 3. Critical Information Value Matrix, continued

US		HI	MED HI	MED	MED LOW	LOW
ADVERSARY		Loss of CI will have a SEVERE impact on our ability to accomplish the mission	Loss of CI will probably have a SERIOUS impact on our ability to accomplish the mission	Loss of CI will likely have an APPRECIABLE impact on our ability to accomplish the mission	Loss of CI will possibly have a MODERATE impact on our ability to accomplish the mission	Loss of CI could have a MINOR impact on our ability to accomplish the mission
MED HI	Of CRUCIAL importance to an adversary that obtaining the information APPRECIABLY contributes to meeting adversary objectives	MED HI	MED HI	MED HI	MED	MED
MED	Of ESSENTIAL importance to an adversary that obtaining the information GREATLY contributes to meeting adversary objectives	MED HI	MED	MED	MED LOW	LOW
MED LOW	Of MODERATE importance to an adversary that obtaining the information contributes to meeting adversary objectives	MED HI	MED LOW	MED LOW	LOW	LOW

Table 3. Critical Information Value Matrix, continued

US		HI	MED HI	MED	MED LOW	LOW
ADVERSARY		Loss of CI will have a SEVERE impact on our ability to accomplish the mission	Loss of CI will probably have a SERIOUS impact on our ability to accomplish the mission	Loss of CI will likely have an APPRECIABLE impact on our ability to accomplish the mission	Loss of CI will possibly have a MODERATE impact on our ability to accomplish the mission	Loss of CI could have a MINOR impact on our ability to accomplish the mission
LOW	Of MINOR importance to an adversary	MED HI	LOW	LOW	LOW	LOW

3. STEP 2 – THREAT MATRIX. Step 2 measures the threat posed by a specific adversary based on the adversary's (or adversaries') known capabilities and intent to collect. Based on the scale in Table 4, assign a value from high to low for the threat severity of known adversaries.

Table 4. Threat Value Matrix

INTENT	CAPABILITY						
	ADVERSARY		HI The adversary's collection is highly developed and MOST LIKELY in place OR the adversary receives equivalent data collection support from a HIGHLY capable 3rd party	MED HI The adversary's collection capability is significantly developed and PROBABLY in place OR the adversary receives equivalent data collection support from a SIGNIFICANTLY capable 3rd party	MED The adversary's collection capability is possibly developed and LIKELY in place OR the adversary receives equivalent data collection support from a CAPABLE 3rd party	MED LOW The adversary's collection capability is probably not developed and MOST LIKELY NOT in place OR the adversary may receive equivalent data collection from a 3rd party	LOW The adversary collection capability is NOT developed OR does NOT receive data support from a 3rd party
	HI	The adversary is HIGHLY motivated and a successful outcome SIGNIFICANTLY contributes to meeting adversary objectives	HI	MED HI	MED HI	MED	MED LOW
	MED HI	The adversary is SIGNIFICANTLY motivated and a successful outcome GREATLY contributes to meeting adversary objectives	MED HI	MED HI	MED HI	MED	LOW

Table 4. Threat Value Matrix, continued

			CAPABILITY				
			HI	MED HI	MED	MED LOW	LOW
	ADVERSARY		The adversary's collection is highly developed and MOST LIKELY in place OR the adversary receives equivalent data collection support from a HIGHLY capable 3rd party	The adversary's collection capability is significantly developed and PROBABLY in place OR the adversary receives equivalent data collection support from a SIGNIFICANTLY capable 3rd party	The adversary's collection capability is possibly developed and LIKELY in place OR the adversary receives equivalent data collection support from a CAPABLE 3rd party	The adversary's collection capability is probably not developed and MOST LIKELY NOT in place OR the adversary may receive equivalent data collection from a 3rd party	The adversary collection capability is NOT developed OR does NOT receive data support from a 3rd party
INTENT	MED	The adversary is SUFFICIENTLY motivated and a successful outcome WILL contribute to meeting adversary objectives	MED HI	MED	MED	MED LOW	LOW
	MED LOW	The adversary is MODERATELY motivated and a successful outcome CAN contribute to meeting adversary objectives	MED	MED LOW	MED LOW	MED LOW	LOW

Table 4. Threat Value Matrix, continued

INTENT	CAPABILITY						
	ADVERSARY		HI	MED HI	MED	MED LOW	LOW
			The adversary's collection is highly developed and MOST LIKELY in place OR the adversary receives equivalent data collection support from a HIGHLY capable 3rd party	The adversary's collection capability is significantly developed and PROBABLY in place OR the adversary receives equivalent data collection support from a SIGNIFICANTLY capable 3rd party	The adversary's collection capability is possibly developed and LIKELY in place OR the adversary receives equivalent data collection support from a CAPABLE 3rd party	The adversary's collection capability is probably not developed and MOST LIKELY NOT in place OR the adversary may receive equivalent data collection from a 3rd party	The adversary collection capability is NOT developed OR does NOT receive data support from a 3rd party
	LOW	The adversary is NOT motivated to collect information	MED LOW	LOW	LOW	LOW	LOW

4. STEP 3 – VULNERABILITY VALUE. Step 3 measures the susceptibility of critical information to adversary collection. This step includes the identification of indicators that can also induce a susceptibility to adversary collection. Based on the scale in Table 5, assign a value from high to low for each vulnerability (and indicator) according to the likelihood it would offer an opportunity for exploitation.

Table 5. Vulnerability Values

HI	Exploitation of this vulnerability by an adversary will make critical information susceptible to at least one intelligence collection discipline virtually any time the adversary chooses to collect.
MED HI	Exploitation of this vulnerability by an adversary will make critical information susceptible to at least one intelligence collection discipline most of the time the adversary chooses to collect.
MED	The adversary's capability to exploit this vulnerability is not well developed but could frequently make critical information susceptible to at least one intelligence collection discipline.
MED LOW	The adversary's capability to exploit this vulnerability is poorly developed, and critical information is only occasionally susceptible to at least one intelligence collection discipline.
LOW	Potential for exploitation is negligible.

5. STEP 4 – RISK ASSESSMENT. Step 4 brings the entire process together. Risk is assessed as a measure of the probability that an adversary will be successful in collecting critical information and the resultant cost to the mission (impact).

a. Probability is determined by multiplying a vulnerability value by the relative threat value. In other words, if the vulnerability involves susceptibility to HUMINT collection, the threat value would be specific to the adversary's HUMINT collection capability. In a situation where a single vulnerability might be exploited by multiple collection methodologies, use the highest rating for risk calculation.

b. Use Table 6 as a decision chart for probability, combining the values for threat and vulnerability.

Table 6. Probability of Critical Information Loss (Threat Severity X Vulnerability Level)

Threat / Vulnerability	HI	MED HI	MED	MED LOW	LOW
HI	HI	MED HI	MED	MED LOW	LOW
MED HI	MED HI	MED	MED	MED LOW	LOW
MED	MED	MED	MED	LOW	LOW
MED LOW	MED LOW	MED LOW	LOW	LOW	LOW
LOW	LOW	LOW	LOW	LOW	LOW

c. Determine the risk by multiplying probability times impact. The measure of impact in this example can be determined by reviewing the value of the critical information that is susceptible to HUMINT collection. Should multiple items of critical information be susceptible to exploitation by a given vulnerability, the analyst makes a decision on the combined value of that critical information. Most often, the combined value is the highest value placed on any one critical information item. For example, if the threat is high and the vulnerability is medium high,

the probability of compromise is medium high. If the threat probability is medium high and the value of the critical information is medium high, the risk is medium.

d. Use Table 7 as a decision chart for risk, combining the values for probability and impact.

Table 7. Risk Assessment

Probability / Impact (CI Value)	HI	MED HI	MED	MED LOW	LOW
HI	HI	MED HI	MED	MED LOW	LOW
MED HI	MED HI	MED	MED	MED LOW	LOW
MED	MED	MED	MED	LOW	LOW
MED LOW	MED LOW	MED LOW	LOW	LOW	LOW
LOW	LOW	LOW	LOW	LOW	LOW

6. STEP 5 – COUNTERMEASURES. Step 5 applies countermeasures to reduce vulnerabilities or threats. Anything to effectively control or hide indicators and reduce the adversary's ability to exploit a vulnerability is an acceptable countermeasure. In identifying and selecting countermeasures, consider cost, time, and effort as well as how much the countermeasure will lower the risk.

Table 8. Risk Assessment Process Example

CRITICAL INFORMATION		ASSUME THE COMMANDER HAS ESTABLISHED AN ACCEPTABLE RISK OF MEDIUM	THREAT[1]	
1. Mission Times	MED HI		SIGINT	HI
2. Security Procedures	MED HI		HUMINT	HI
3. Specific Logistics Support	MED HI		GEOINT	MED HI
4. Crew Names With Missions	HI		OSINT	MED
5. Assets Assigned to Missions	HI		MASINT	MED LO

Vulnerability and/or Indicator		Probability[2]	Impact[3]	Risk	Countermeasure[4]	Residual Risk[5]
Use of open networks	HI	HI	HI	HI	Restrict coordination of mission activities to classified networks. Reduces the vulnerability to medium	MED
Use of commercial shipping	MED HI	MED HI	HI	MED HI	None immediately available	MED HI[6]

Table 8. Risk Assessment Process Example, continued

CRITICAL INFORMATION		ASSUME THE COMMANDER HAS ESTABLISHED AN ACCEPTABLE RISK OF MEDIUM			THREAT[1]	
1. Mission Times		MED HI			SIGINT	HI
2. Security Procedures		MED HI			HUMINT	HI
3. Specific Logistics Support		MED HI			GEOINT	MED HI
4. Crew Names With Missions		HI			OSINT	MED
5. Assets Assigned to Missions		HI			MASINT	MED LO
Vulnerability and/or Indicator		Probability[2]	Impact[3]	Risk	Countermeasure[4]	Residual Risk[5]
Crew member personal information on official Web pages	HI	MED	HI	MED	Bring unit Web pages into compliance with DoD policy. Conduct unit awareness. Reduces the vulnerability to medium	MED
Stereotyped operations	MED	MED	HI	MED	None required	

[1] In this example, assume two adversaries with different intents and capabilities. The value entered here is the combined threat from both adversaries using the highest of the values. For instance, adversary 1 represents a medium SIGINT threat and adversary 2 represents a high SIGINT threat. High is used for the risk analysis. Adversary 1 represents a high HUMINT threat and adversary 2 represents a medium high HUMINT threat. High is used for the risk analysis.

[2] Use of open networks is susceptible to SIGINT; high threat times high vulnerability equals high probability. Use of commercial shipping makes critical information susceptible to SIGINT, HUMINT, GEOINT, and OSINT; the highest threat value is high, so high threat times medium high vulnerability equals medium high probability.

[3] Use of open networks could place all of the critical information at risk. The combined impact of the adversary's exploitation of that critical information would be high. Use of commercial shipping could potentially place critical information items 3 and 5 at risk, with an impact value of high.

[4] If the commander's acceptable risk level is medium and the initial risk analysis is medium, no countermeasure is required. However, if a remedy is readily available and inexpensive, a countermeasure may still be recommended.

[5] By reducing the vulnerability to medium, the probability of exploitation is reduced to medium; medium times high impact equals medium risk.

[6] There may not always be an effective countermeasure available to reduce the vulnerability or otherwise mitigate the risk. By identifying this, the commander may determine whether that vulnerability is acceptable or may determine that more expensive countermeasures, or a change in the plan, might be warranted.

ENCLOSURE 5

INFORMATION PROTECTION REQUIREMENTS

1. CONTENT REVIEWS. This section supplements guidance related to the release of information in DoDD 5230.09 (Reference (e)), DoD Instruction (DoDI) 5230.29 (Reference (f)), and Deputy Secretary of Defense Memorandum (Reference (g)). A content review is an evaluation of information intended for release outside the control of the organization, including release to the public. OPSEC focuses on identifying and protecting the organizations unclassified information that may individually or in the aggregate lead to the compromise of classified information and sensitive activities.

a. The OPSEC program manager or coordinator will work closely with public affairs, information security, Web administrators, and other officials designated by the DoD Component who also share responsibility for the release of information. Commanders and directors are responsible for ensuring there is a valid mission need to disseminate the information and that review procedures are implemented.

b. The Heads of the DoD Components shall develop, establish, and implement policies and procedures to deny adversaries the opportunity to take advantage of publicly available information, especially when aggregated. Policies and procedures shall include:

(1) A formal review of content for its sensitivity (e.g., critical information, For Official Use Only, or other controlled unclassified information categories), sensitivity in the aggregate, determination of appropriate and/or intended audience, and distribution and release controls.

(2) The designation of individuals who have received the appropriate training in OPSEC, security, and release requirements to be responsible for reviewing information intended for public release, or the inclusion of the OPSEC program manager or coordinator as part of the formal review process.

(3) Consideration of the method by which the information will be distributed, susceptibility of the information to data mining, and the likelihood that the information could lead directly to the discovery and display of knowledge that is otherwise controlled. The ease with which data can be transferred to another media or distributed by another method should also be considered.

(4) The requirement that release of information on DoD (or DoD Component) Web sites and Web-based applications shall be in accordance with Reference (g). Release officials shall consider the intended audience and appropriate Web domain (e.g. publicly accessible, government restricted, internal to the DoD Component) and shall restrict the information to that domain.

2. INFORMATION SYSTEMS. Automated information systems allow for the compilation of large quantities of data or help to facilitate interoperability of systems that enable data aggregation. Compilation or aggregation of data may lead to OPSEC or classification issues.

a. System owners shall address OPSEC and information security during initial planning stages. Information security managers, systems security, information assurance, and OPSEC personnel shall be engaged during initial planning and definition stages to advise on classification, assess vulnerabilities and risks, and provide guidance on mitigation strategies.

b. The DoD Components shall review those information systems or applications and/or programs designed for net-centric interoperability for data aggregation and classification issues in accordance with DoD 5200.1-R (Reference (h)). The DoD Components shall engage security and information assurance experts and integrate security options when developing new systems, applications, and net-centric environments (such as collaboration portals, data sharing environments, data mining tools, and other tools that aggregate or permit the aggregation of large quantities of data).

3. HANDLING REQUIREMENTS

a. Handling and Safeguarding. Information that has been identified by the DoD Component as critical information should be handled accordingly. Components shall provide guidance on handling and safeguarding requirements for critical information.

b. Destruction. The preferred method to destroy critical information is by shredding or burning. If these methods are not available critical information shall be destroyed in a manner that prevents routine recognition or reconstruction.

ENCLOSURE 6

CONTRACT REQUIREMENTS

1. INTRODUCTION

a. Commanders and directors shall ensure that contractors supporting DoD activities use OPSEC to protect critical information for specified contracts and subcontracts. The requiring organization and Government Contracting Activity (GCA) shall impose OPSEC measures as contractual requirements when necessary.

b. It is the requiring organization's responsibility to:

(1) Determine what OPSEC measures and requirements are essential to protect critical information for specific contracts.

(2) Identify those OPSEC measures in their requirements documents.

(3) Ensure the GCA identifies those OPSEC measures and requirements in the resulting solicitations and contracts.

2. PROCEDURES

Heads of the DoD Components shall establish procedures to ensure that contract requirements properly reflect OPSEC responsibilities and that those responsibilities are included in both classified and unclassified contracts when appropriate.

a. Requiring organizations must determine if there is critical information associated with the contract or activities involved in the contract that warrants the inclusion of OPSEC requirements. Consideration shall be given to the type of work being performed and the environment and circumstances in which contract performance will occur. In some cases, contractors may simply be required to receive threat awareness briefings or basic security training for employees.

b. If OPSEC requirements are necessary, an OPSEC review shall be conducted of the statement of work (SOW) for classified and unclassified contracts prior to the time the GCA releases the SOW to contract bidders. The SOW is a publicly released document that can reveal critical information or indicators of critical information. It is important that GCAs work with their OPSEC program managers and coordinators to identify OPSEC requirements for the scope of work to be performed. The SOW should also undergo a formal content review prior to its release to the public.

c. Requirements for OPSEC must be included in the contract solicitation and resulting contract in sufficient detail to ensure complete contractor understanding of all OPSEC provisions required. OPSEC requirements levied on contractors may include but are not limited to:

(1) Specific OPSEC measures the contractor is required to follow.

(2) Specific OPSEC awareness training.

(3) Participation in the command or unit OPSEC program.

(4) Development of an OPSEC program with specific features based on command- or unit-approved OPSEC requirements.

d. For classified contracts, the command or unit and GCA will specify OPSEC requirements on DD Form 254, "Department of Defense Contract Security Classification Specification." OPSEC requirements apply to National Industrial Security Program (NISP) contractors when it is determined that additional safeguards are essential for specific contracts; they are imposed in addition to the standard requirements of the NISP.

(1) The command or unit will state OPSEC requirements on the DD Form 254 in sufficient detail to ensure complete contractor understanding of the exact OPSEC provisions or measures required. Full disclosure of these requirements is essential so that contractors can comply and charge attendant costs to the specific contracts for which these measures have been ordered.

(2) If the command or unit requires the contractor to adhere to the command or unit OPSEC requirements, the DD Form 254 must have OPSEC checked as a requirement. The contractor must also be provided with a copy of the command or unit OPSEC requirements or plan.

(3) Commands and units shall ensure contractors do not disclose classified or unclassified information pertaining to a classified contract to the public without prior review and clearance as specified in the requirements in block 12 of the DD Form 254.

(4) Commands and units shall assist the Defense Security Service in ensuring adequacy of industrial security efforts for OPSEC applied to classified contracts in accordance with DoD 5220.22-R (Reference (i)).

ENCLOSURE 7

OPSEC EDUCATION, TRAINING AND AWARENESS

1. INTRODUCTION

a. In accordance with Reference (a), OPSEC education and training is required for personnel assigned OPSEC responsibilities. Awareness training shall be provided to the work force.

b. OPSEC education and training may be accomplished through establishing programs within the DoD Component, using external resources such as the IOSS and the Defense Security Service Academy, or a combination.

c. The objectives of OPSEC education, training, and awareness shall be to:

(1) Provide necessary knowledge, skills, and information to enable quality performance of OPSEC functions.

(2) Promote understanding of OPSEC program policies and requirements and their importance to overall security.

(3) Instill and maintain within the DoD workforce a continuing awareness of OPSEC requirements and the intelligence threat.

(4) Assist in promoting a high degree of motivation to support program goals.

2. EDUCATION AND TRAINING. All personnel assigned to OPSEC-related duties must satisfy both preparatory and sustaining DoD standard education and training requirements upon assignment. Heads of the DoD Components shall use the IOSS certification program or DoD Component equivalent for individuals appointed OPSEC duties.

a. OPSEC Program Managers. All OPSEC program managers who have OPSEC duties as their primary job shall complete the OPSEC Fundamentals Course within 30 days of assignment. Within 90 days of assignment, all OPSEC program managers shall attend the IOSS program manager course or other DoD Component equivalent course.

b. OPSEC Coordinators. All OPSEC coordinators who have OPSEC duties as part of their job shall complete the OPSEC Fundamentals Course within 30 days of assignment. Components shall determine additional OPSEC education and training requirements.

c. Information Operations (IO) Career Force

(1) The Heads of DoD Components shall submit proposed (joint) education curriculum for IO career force personnel to the IO Education Board of Advisors for approval in accordance with DoDI 3608.12 (Reference (j)). Upon approval, the Heads of DoD Components shall establish OPSEC education and training requirements for IO career force personnel in Component guidance.

(2) For DoD Component-only IO courses, the DoD Components shall at a minimum include the following OPSEC objectives as part of IO education and training.

(a) Understand the OPSEC process and provide a general knowledge of OPSEC, threats, vulnerabilities, and individual responsibilities for protecting critical information.

(b) Demonstrate how OPSEC integrates with other core, supporting, and related capabilities of IO from mission and operations conception through post mission and operation actions.

(c) Explain the relationship of DoD Component OPSEC to joint OPSEC.

3. AWARENESS TRAINING

a. All personnel in the organization shall be provided an initial orientation to the organization's OPSEC program. This initial orientation is intended to provide employees a degree of understanding of OPSEC policies and doctrine commensurate with their responsibilities.

b. Initial orientation at a minimum shall include an explanation of OPSEC, its purpose, threat awareness, the organization's critical information, and the individual's role in protecting it. General organizational orientations may need to be supplemented by duty-related orientations in the work center targeted toward specific critical information and vulnerabilities associated with the work.

c. OPSEC education should be continuous rather than periodic. Briefings, awareness sessions, and other formal presentations should be supplemented with other information and promotional efforts to ensure maintenance of awareness and understanding of both adversary threat and of the techniques employed by adversaries to collect classified and sensitive information. The circulation of directives or similar material on a "read and initial" basis shall not be utilized as a sole means of fulfilling any of the specific requirements of this enclosure.

d. As a minimum, all personnel shall receive annual refresher OPSEC training that reinforces understanding of OPSEC policies and procedures, critical information, and procedures covered in initial and specialized training. Refresher training should also address the threat and techniques employed by adversaries attempting to obtain classified and sensitive information.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

DoDD	DoD Directive
DoDI	DoD Instruction
DoDM	DoD Manual
GCA	Government Contracting Activity
GEOINT	geospatial intelligence
HUMINT	human intelligence
IO	information operations
IOSS	Interagency OPSEC Support Staff
MASINT	measurement and signature intelligence
NISP	National Industrial Security Program
OPSEC	operations security
OSINT	open-source intelligence
SIGINT	signals intelligence
SOP	standard operating procedures
SOW	statement of work

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this Manual.

adversary. An individual, group, organization, or government that must be denied critical information.

CIL. A list of critical information that has been fully coordinated within an organization and approved by the senior decision maker, and is used by all personnel in the organization to identify unclassified information requiring application of OPSEC measures.

CIP. Defined in Reference (d).

countermeasure. Anything that effectively negates or mitigates an adversary's ability to exploit vulnerabilities.

critical information. Defined in Joint Publication 1-02 (Reference (k)).

indicator. Data derived from friendly detectable actions and open-source information that adversaries can interpret and piece together to reach conclusions or estimates of critical or classified information concerning friendly intentions, capabilities, or activities.

IO. Defined in Reference (k).

OPSEC. Defined in Reference (a).

OPSEC assessment. Defined in Reference (a).

OPSEC coordinator. Defined in Reference (a).

OPSEC measure. Defined in Reference (k).

OPSEC plan. A plan that provides the organization a living document that can be used to implement the appropriate countermeasures given the mission, assessed risk, and resources available to the unit. OPSEC plans generally take two forms; both should be updated as circumstances and personnel change over time.

An OPSEC operations plan provides specific countermeasures to be applied in a specific operation. It may be generated as an annex to a Joint Operation Planning and Execution System plan or as a local document endorsed by the commander.

An OPSEC program plan provides guidelines for implementation of routine procedures and measures to be employed during daily operations or activities of a given unit. The plan should be endorsed by the unit commander.

OPSEC process. A process that examines a complete activity to determine what, if any, exploitable evidence of classified or sensitive activity may be acquired by adversaries. It is an analytical, risk-based process that incorporates five distinct elements.

Critical information identification.

Threat analysis.

Vulnerability analysis.

Risk assessment.

OPSEC countermeasures.

OPSEC program manager. Defined in Reference (a).

OPSEC survey. Defined in Reference (a).

risk. A measure of the potential degree to which protected information is subject to loss through adversary exploitation.

risk assessment. A process of evaluating the risks to information based on susceptibility to intelligence collection and the anticipated severity of loss.

risk management. The process of identifying, assessing, and controlling risks by making decisions that balance risk costs with mission benefits. Costs may be measured in financial cost, loss of assets, loss of information, or loss of reputation.

sensitive information. Information that the loss, misuse, unauthorized access, or modification could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (Reference (l)), but that has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of National defense or foreign policy.

threat analysis. A process that examines an adversary's technical and operational capabilities, motivation, and intentions, designed to detect and exploit vulnerabilities.

vulnerability analysis. A process that examines a friendly operation or activity from the point of view of an adversary, seeking ways in which the adversary might determine critical information in time to disrupt or defeat the operation or activity.