



Interagency OPSEC Support Staff

Meeting the Challenges of a Changing World

[[OPSE-1300](#)] [[OPSE-1301](#)] [[OPSE-1500](#)] [[OPSE-2380](#)] [[OPSE-2390](#)]
[[OPSE-2400](#)][[OPSE-3100](#)] [[OPSE-3500](#)] [[Public Safety](#)]

Standard Courses

OPSE-1300, Operations Security Fundamentals▲

Prerequisite: None

Length: 1 day

Delivery Mode: Platform instruction and video teleconference available.

CY2006 Schedule: Available only from the Mobile Training Team

**OPSE-1300 will not be on the calendar after this session, but will be available as a mobile training team (MTT) to any customer location provided customer is prepared to pay travel and per diem expenses for the instructor. [OPSE-1301, OPSEC Fundamentals CD](#), the computer-based training version of this course, is available on CD and may be ordered from the IOSS.*

Description: This course provides a basic working knowledge of OPSEC as outlined in National Security Decision Directive (NSDD) 298. Lectures focus on understanding how OPSEC principles are used in the workplace, especially in the law enforcement; military; research,

development, testing and engineering (RDT&E) and acquisition communities.

Requires a U.S. SECRET Clearance. Courses taught under a mobile training agreement can be taught at the unclassified level.

Target student population: This course is useful for those who need a familiarity with the OPSEC process, to include managers and executives.

OPSE-1500, OPSEC and Web Content Vulnerability ▲

Prerequisite: None

Length: 2 days

Method of instruction: Platform instruction

FY2007 Schedule: Oct 2-3, Jan 8-9, Mar 12-13, Jun 4-5, Aug 13-14

Description: This course addresses the OPSEC issues that should be considered when reviewing information for public release. Lessons from this course can be applied to preparing information for release in all forms of media, including print, news articles, web publication, or public speeches. It is a two day seminar featuring high level guest speakers from government and military, making presentations on lessons learned from their perspectives.

Objective: After completing this course, the student will be able to:

- Describe content problems in released information
- Describe how the OPSEC process applies to the public release of information

Requires a U.S. SECRET Clearance. Courses taught under a mobile training agreement can be taught at the unclassified level.

Target student population: This course is specifically designed for individuals who are involved in determining what information would be released to the public, such as public affairs staff, web masters, or FOIA review staff, or anyone who sends e-mail or surfs the Web.

Note: *This is an OPSEC fundamentals-level course. Course materials are tailored to the target student population.*

OPSE-2380, OPSEC Analysis Course ▲

Prerequisite: OPSE-1301, OPSEC Fundamentals CBT or other equivalent fundamentals training

Length: 3 days

Method of instruction: Platform instruction

FY2007 Schedule: Oct 16-18, Dec 4-6, Jan 22-24, Mar 5-7, Apr 23-25, Jun 11-13, Jul 9-11, Sep 10-12

Description: The focus of this course is on the basic skills and knowledge needed by the OPSEC practitioner.

Objective: Upon completing this course, students will be able to:

- Apply the systems analysis methodology to their own organizations and activities
- Identify sources of information and support materials for OPSEC practitioners
- Conduct an OPSEC analysis of a program, activity or operation, including:
 - Tools for identification of critical information
 - Analysis of threat and resources to obtain threat information
 - Using the web for threat analysis
 - Identification of vulnerabilities, including the most common problem areas
 - Analysis of risk
 - Development and implementation of countermeasures, and assessment of residual risk
 - Communicating analysis to leadership

Requires a U.S. SECRET Clearance. Courses taught under a mobile training agreement can be taught at the unclassified level.

Target student population: This course is designed for individuals performing OPSEC analysis, such as OPSEC coordinators, working group members, and security personnel.

OPSE-2390, OPSEC Program Manager's Course ▲

Prerequisite: OPSE-2380, OPSEC Analysis Course or other equivalent training

Length: 2 days

Method of instruction: Platform instruction

FY2007 Schedule: Oct 19-20, Dec 7-8, Jan 25-26, Mar 8-9, Apr 26-27, Jun 14-15, Jul 12-13, Sep 13-14

Description: The focus of this course is on the basic skills and knowledge needed to implement an OPSEC program. The student is afforded the opportunity to apply OPSEC tools and lessons through a variety of practical exercises and case studies.

Objective: Upon completing this course, students will be able to:

- Market an OPSEC program
- Brief management
- Define OPSEC management boundaries
- Write an OPSEC policy
- Implement and monitor an OPSEC program
- Lead a working group
- Establish an OPSEC network

Requires a U.S. Secret Clearance.

Target student population: This course is specifically designed for individuals assigned OPSEC officer, OPSEC working group or OPSEC program manager duties, who will be responsible for an OPSEC program and application of the OPSEC process to the organization's activities.

OPSE-2400, DoD OPSEC Course ▲

This course of instruction has been moved from the IOSS to the DSS Training Academy, Lithicum MD

To Register Go to www.dss.mil click on "DSS Academy" Then click on "ENROL" Then follow the instructions on the screen.

Prerequisite: OPSE-1301, OPSEC Fundamentals CBT or other equivalent fundamentals training. Also, a pre-course worksheet is sent to students when they register for the course; registration closes one month prior to each course. Students wishing to register within the one-month-prior window must have the permission of the instructor.

All students must order prerequisite materials from the IOSS Website, before reporting to this course of instruction. (i.e, Intelligence Threat Handbook, Terrorism Threat Handbook, & OPSE 1301 CBT)

Length: 5 days

Method of instruction: Platform instruction with mentor-supervised individual project work

FY2007 Schedule: Oct 23-27 (Lackland AFB, TX), Jan 22-26 (Lackland AFB, TX), Feb 26-2Mar (Hurlbert Field, FL)
Mar 19-23 (NIOC San Diego), Apr 9-13 & July 23-27 (DSS Academy, Lithicum, MD), Sep 24-28 (NIOC Norfolk,VA)

Description: This course is designed to prepare DoD OPSEC personnel to provide OPSEC planning and analysis support to their commanders, to develop and implement an OPSEC program within an organization, and to plan OPSEC assessments. Students are assigned a mentor, and work on their own unit program in place of a fictitious scenario. The IOSS presents this course in partnership with the Department of Defense.

Objective: Upon completing this course, students will be able to:

- Support the JOPES process
- Identify critical information
- Perform threat analysis
- Identify vulnerabilities
- Analyze risk
- Develop and implement countermeasures, assessing residual risk
- Develop OPSEC awareness programs and materials for their workforce(s)
- Write an OPSEC program plan
-

Requires a U.S. SECRET Clearance. Courses taught under a mobile training agreement can be taught at the unclassified level

Target student population : This course is designed specifically for DoD personnel. Non-DoD students must have the permission of the DoD OPSEC Program Manager to attend the course; contact the IOSS registrar at 443-479-4671 for more information.

Note: *Personnel who have attended the OPSEC Analysis and OPSEC Program Manager's Course will find the material presented in this course redundant.*

OPSE-3100, Advanced OPSEC Applications Course ▲

Prerequisite: OPSE-2380, OPSEC Analysis Course or other equivalent training (incorporates the former OPSE-2330 Threat Analysis Course)

Length: 4 days

Method of instruction: Platform instruction

FY2007 Schedule: Nov 14-16 (**Cancelled**), Feb 13-15, Apr 2-5, Sep 18-20

Description: This course provides detailed instruction on skills critical to the professional practice of OPSEC. Main topics of the course are common vulnerabilities, developing threat information for OPSEC analysis, use of the internet and conducting OPSEC surveys. Other subjects addressed include the Freedom of Information Act, classification management, and red teaming.

Objective: Upon completing this course, students will be able to:

- Perform open source research
- Identify common security issues
- Obtain threat information, to include writing a request for information, who to ask, how to ask and what to ask for
- Recognize the most common OPSEC vulnerabilities
- Implement appropriate countermeasures to reduce risk
- Perform a survey, including organizing a survey team, administrative issues, information gathering, interviewing techniques, and analysis and reporting

Requires a U.S. Secret Clearance.

Target student population: This course is specifically designed for individuals assigned as OPSEC coordinators or OPSEC program managers.

OPSE-3500, Web Risk Assessment Course ▲

Prerequisite: OPSE-1301, OPSEC Fundamentals CBT or other equivalent fundamentals training

Length: 3 days

Method of instruction: Platform instruction

FY2007 Schedule: Jan 10-12, Mar 14-16, Jun 6-8, Aug 15-17

Description: Principles of reviewing web pages for OPSEC vulnerabilities are the primary subject of this course. Use of checklists, commercially available software, and government-developed software are addressed as evaluation and review techniques. The course

also provides an overview of the nature and use of the internet to give the student an appreciation of why release of information on a web page might represent an unanticipated risk.

Requires a U.S. Secret Clearance.

Target student population: This course is specifically designed for individuals who are involved in evaluating official web pages. Graduates of the Editing for the Web course who desire a more advanced look at the issues of public release will also benefit from this course. NOTE: Students who have attended Advanced OPSEC Applications may find this material redundant.

OPSEC for Public Safety Course (not yet accredited by NCS) ▲

Prerequisite: None

Length: 3 days

Method of instruction: Platform instruction

This course has been transferred to the Federal Law Enforcement Training Center Glynco GA (FLETC) effective April 1, 2006 for registration [Click here!](#)

Students who successfully complete the training will be able to apply OPSEC to emergency and special event planning; special operations such as SWAT, HazMat, WMD, Bomb Squad; intelligence, counter terrorism, arson, and narcotics task forces; and criminal investigations. Course instructors have public safety, security, and intelligence backgrounds. The IOSS presents this course in partnership with the Department of Homeland Security OPSEC program.

Target student population: This course is designed specifically for U.S. agencies with a law enforcement, emergency management, fire and rescue, and infrastructure protection mission. Non-credentialed students must have the permission of the DHS OPSEC Program Manager to register for the course; contact the IOSS registrar at 443-479-4671 for more information.

Computer-based Training Course

The IOSS currently offers one computer-based training (CBT) course. IOSS is reviewing all IOSS courses for future CBT consideration.

OPSE-1301, OPSEC Fundamentals CBT ▲

Prerequisite: None

Length: 2 to 4 hours

Method of instruction: Self-paced computer-based instruction

Description: This course is designed to provide students with a basic working knowledge of OPSEC and how it applies to executive branch agencies and departments. The course focuses on the history of OPSEC and the OPSEC process as described in NSDD-298.

Objective: After taking this course, the student will be able to apply the systems analysis methodology.

Target student population: Unit personnel who require knowledge of the OPSEC process, but who will not be asked to perform OPSEC analysis, including managers, working group members, and OPSEC coordinators supporting the unit OPSEC program.

This CBT can be ordered from the IOSS website