

31 MAY 2001



Operations

OPERATIONS SECURITY

NOTICE: This publication is available digitally on the AFDPO WWW site at:
<http://afpubs.hq.af.mil>.

OPR: HQ USAF/XOIWI
(Capt Eric M. Lambert)
Supersedes AFD 10-11, 17 May 1993.

Certified by: HQ USAF/XO
(Lt Gen Robert H. Foglesong)
Pages: 4
Distribution: F

This policy directive provides guidance for planning and conducting Operations Security (OPSEC). This policy applies to all military and civilian personnel, members of the Air Force Reserve, Air National Guard, DoD contractors, and individuals or activities under legal agreement or obligation with the Department of the Air Force.

SUMMARY OF REVISIONS

The primary need to update this AFD stems from publication of AFD 10-20, Defensive Counterinformation Operations and the integration of the Operations Security (OPSEC) process into information operations (IO). The update also includes new reporting requirements, integration of OPSEC into Force Protection/Antiterrorism, and updates office symbols resulting from Air Staff reorganization.

- 1.** Operations Security (OPSEC) is a component of information operations (IO) that increases the Air Force's effectiveness by reducing mission vulnerabilities. OPSEC requires very close integration with the various security programs and other aspects of IO. Its objective is to assist operators at all levels to achieve information superiority and carry out effective and successful missions. As a component of Force Protection and Antiterrorism OPSEC helps to protect service members, civilian employees, family members, facilities and equipment in all locations and situations. OPSEC provides a methodology to identify and protect critical information potential adversaries could exploit.
- 2.** To prevent an adversary from gaining a military advantage, the Air Force must avoid inadvertent or premature disclosure of critical information. The Air Force will use the OPSEC process to identify and control information of potential value to an adversary.
- 3.** OPSEC is a command responsibility. Air Force commanders will take an active role to ensure the successful application of their OPSEC program.
 - 3.1.** Commanders at every level will establish a program that ensures OPSEC is fully integrated into their mission responsibilities. Personnel under their command must understand what information is

critical; how they are to protect it; from whom they are to protect it; and for how long they must protect it.

4. This directive establishes the following responsibilities and authorities:

4.1. The Deputy Chief of Staff for Air and Space Operations (HQ USAF/XO) is the office of primary responsibility for the Air Force OPSEC program. HQ USAF/XO will designate a full-time Air Staff OPSEC Program Manager (PM) to develop policy and influence plans.

4.2. Major Commands (MAJCOM), field operating agencies (FOA), and direct reporting units (DRU) will develop effective and visible OPSEC programs to satisfy mission requirements as detailed in AFI 10-1101, Operations Security (OPSEC) Instruction.

4.2.1. MAJCOMs, FOA's, DRU's, laboratories, products and logistics centers, and test ranges will assign at least one commissioned officer (or civilian grade equivalent) to function as the OPSEC PM. The PM should be a full-time responsibility. The PM position should be assigned to the element of an organization that maximizes integration into critical mission areas.

4.2.2. Effective OPSEC programs will identify critical information; assess the intelligence collection threat; ensure job-related and mission-specific training is provided on a recurring basis to all personnel; ensure the integration of OPSEC measures with supporting units; and conduct annual OPSEC appraisals and reports IAW AFPD 10-20.

4.2.3. In the acquisition environment, the PM should work directly with the program director to ensure OPSEC principles are integrated and applied throughout the life-cycle of all programs.

4.3. Air Force Information Warfare Center (AFIWC) is the center of expertise for functional OPSEC training. AFIWC will conduct OPSEC Multi-Discipline Vulnerability Assessment (OMDVA) surveys as part of IO red teaming. Air Force Office of Special Investigations (AFOSI) is the focal point for counterintelligence support and will augment OPSEC surveys and IO red teams by assessing the human intelligence (HUMINT) collection threat.

4.4. AFOSI and Air Intelligence Agency will provide an analysis of the foreign intelligence collection threat to Air Force units and supporting organizations for use in OPSEC planning.

4.5. Air Education and Training Command (AETC) will provide a basic introduction of OPSEC to all initial accession trainees.

4.6. Air University will provide a basic introduction in all professional level courses.

5. See Attachment 1 for publications that implement and interface with this policy.

LAWRENCE J. DELANEY
Acting Secretary of the Air Force

Attachment 1

IMPLEMENTING AND INTERFACING DOCUMENTS

A1.1. This policy implements the following publications:

<u>Publication Designation</u>	<u>Title</u>	<u>Former Publication or Date</u>
DoD Directive 5100.78	United States Port Security Program	25 Aug 86
DoD Directive 5205.2	DoD Operations Security Program	29 Nov 99
Joint Pub 3-54	Joint Doctrine for Operations Security	24 Jan 97
Joint Pub 3-07.2	Joint Tactics, Techniques, and Procedures for Antiterrorism	17 Mar 98
AFPD 10-20	Defensive Counterinformation	No Former Publication
AFDD 2-5	Information Operations Doctrine	5 August 98

A1.2. This policy interfaces with the following publications:

<u>Publication Designation</u>	<u>Title</u>	<u>Former Publication or Date</u>
AFPD 10-7	Command and Control Warfare	No Former Publication
AFI 10-1101	Operations Security (OPSEC) Instructions	AFRs 55-30, 55-32, 55-36, 55-39, and 205-1
AFI 10-1102	Safeguarding the Single Integrated Operational Plan (SIOP)	AFR 205-25
AFI 10-1103	USAF Sensitive Reconnaissance Programs	AFR 55-39
AFI 10-1105	Port Security Program Instructions	AFR 55-32
AFPD 31-7	Acquisition Security	2 Mar 93

<u>Publication Designation</u>	<u>Title</u>	<u>Former Publication or Date</u>
AFI 33-129	Transmission of Information via the Internet	1 Aug 99
AFI 33-219	Telecommunications Monitoring and Assessment Program	15 May 00
AFI 35-101	Public Affairs Policies and Procedures	1 Dec 99