BY ORDER OF THE COMMANDER
30TH SPACE WING

30TH SPACE WING INSTRUCTION 10-102

30 DECEMBER 1998

Operations

THE OPERATIONS SECURITY (OPSEC) PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the30th Space Wing WWW site at: http://vepdl.vafb.af.mil. If you lack access, contact your Publishing Office.

OPR: 30 SW/XPRO (R. J. Edwards)
Supersedes 30 SWI 10-102, 7 November 96.

Certified by: 30 SW/XPRO (R. J. Edwards)
Pages: 5
Distribution: F

This instruction implements AFI 10-1101, ***Operations Security (OPSEC)*** Instruction and establishes an Operations Security Program for the 30th Space Wing (30 SW). It also establishes an OPSEC Manager and OPSEC Monitor function at the Group level. This instruction applies to all 30 SW organizations. Associated tenant organizations shall be expected to participate as will Department of Defense contractor organizations to the extent specified in their respective contract statement of work or DD Form 254, **Contract Security Classification Specification**. See Attachment 1 for a Glossary of References, and Supporting Information. The Paperwork Reduction Act of 1974 as amended in 1996 and AFI 37-160, Volume 8***, The Air Force Publications and Forms Management—Developing and Processing Forms,*** affects this publication.

SUMMARY OF REVISIONS

The revision of this publication is to meet the format standards required by the Air Force. No content material has changed. Some required format changes have been made to allow for the conversion process.

1. Objective. The primary goal of the Wing OPSEC Program is to deny undisclosed information of intelligence value to an adversary which identifies intentions, capabilities, limitations or vulnerabilities which may be exploited to degrade specific mission effectiveness or to provide an unfair business advantage to a competitor over a commercial firm doing business at Vandenberg AFB. The following program objectives must be satisfied in order to meet this goal:

1.1. Incorporate OPSEC planning into day-to-day mission activities. Consider OPSEC in planning compliance with the Strategic Arms Reduction Treaty, Chemical Weapons Convention, and Open Skies treaties.

1.2. Integrate OPSEC into every aspect of the mission. OPSEC must be considered when awarding contracts, reviewing new programs wanting to use Wing resources, protecting financial and personal data, and conducting space, ballistic and aeronautical operations.

1.3. Apply OPSEC processes to determine vulnerabilities/risks and to analyze how well the protective security programs, including telecommunications and computer security programs, provide countermeasures.

1.4. Develop protection standards for sensitive unclassified information and operational data at a minimum cost and impact to mission effectiveness.

1.5. Promote awareness of the adversarial threat to the 30 SW and develop awareness training to counter the threat.

2. Responsibilities.

2.1. The Commander, 30 SW, has overall responsibility for the OPSEC Program.

2.2. The Wing OPSEC Manager is the Plans Office (30 SW/XP) and will implement the Wing OPSEC Program.

2.3. Group commanders will appoint OPSEC managers and monitors.

3. The OPSEC Program.

3.1. The Wing OPSEC Manager (30 SW/XPRO) will:

3.1.1. Establish OPSEC policy and procedure for Vandenberg AFB.

3.1.2. Maintain continuous oversight of the program and measure its effectiveness through staff briefings, assistance visits and program reviews.

3.1.3. Compile and publish list of “Wing Items of Critical Information” for 30 SW/CC approval.

3.1.4. Evaluate contractor compliance with requirements specified in the contractor's statement of work or DD Form 254, **Contract Security Classification Specification**.

3.1.5. Implement a training program, which includes orientation, awareness, and specialized training.

3.1.6. Conduct assessments and surveys of missile and aeronautical operations and other activities that augment or support the mission.

3.1.7. Ensure a capability to obtain intelligence threat information as it pertains to the 30 SW, the Western Range, and its remote sensors, on and off the base, and to military and commercial customers of the Western Range.

3.2. OPSEC managers and OPSEC monitors are established at the Group Level. Associate tenants are expected to participate and to designate OPSEC managers and OPSEC monitors for their organizations. To the extent specified in their DD Form 254**, Contract Security Classification Specification**, contractor organizations will also be expected to participate in the 30 SW OPSEC Program. The number of OPSEC monitors will be determined by the size, complexity and the organizations technical involvement in Wing missile and aeronautical operations, and the diversity of critical technology information handled by the organization.

3.2.1. Group OPSEC managers and monitors must have at least a SECRET security clearance.

3.2.2. Appointment memorandum for designated Group OPSEC **managers** will be sent to the Wing OPSEC Manager (30 SW/XPRO) with a copy retained in the Group's OPSEC manager's continuity folder. Appointment notices for Group OPSEC **monitors** need to be retained in the Group OPSEC managers continuity folder, only.

3.2.3. The Wing OPSEC Manager will provide initial training to newly appointed Group OPSEC managers within 10 days following appointment. Group OPSEC managers will provide initial training to newly appointed OPSEC monitors within 10 days following appointment.

3.3. Group OPSEC Managers will:

3.3.1. Develop "Items of Critical Information" for their respective organizations and will review and update their respective organization's information as changes in mission, operations or programs occur.

3.3.2. Ensure newly assigned personnel are administered a unit "OPSEC Orientation Briefing" within 10 days of assignment to the organization.

3.3.3. Conduct semiannual OPSEC training of assigned personnel. This training will consist of, as a minimum:

3.3.3.1. Briefing of organizations items of critical information.

3.3.3.2. Organizational vulnerabilities, if any.

3.3.3.3. The adversarial threat to the 30 SW (provided by the Wing OPSEC Manager) and the organization.

3.3.3.4. Information, data, or material provided by the Wing OPSEC Manager.

3.3.4. Attend OPSEC meetings called by the Wing OPSEC Manager.

3.3.5. Participate in OPSEC surveys conducted by the Wing OPSEC Manager.

3.3.6. Participate in self-inspection programs.

3.3.7. Create and maintain a continuity OPSEC file, binder, or handbook, which consists of the following information:

3.3.7.1. Memorandums of appointment.

3.3.7.2. Items of critical information.

3.3.7.3. Self-inspection checklist.

3.3.7.4. Training documentation.

3.3.7.5. OPSEC survey documentation.

3.3.7.6. Staff assistance and program review reports.

3.3.7.7. Meeting minutes (internal and external).

3.3.7.8. Threat information.

3.3.7.9. Miscellaneous data.

3.3.7.10. AFPD 10-11, ***Operations Security***.

3.3.7.11. AFI 10-1101, ***Operations Security (OPSEC).***

3.3.7.12. 30 SWI 10-102, ***The Operations Security (OPSEC) Program***.

3.3.7.13. Policy Letters.

3.3.8. Develop and use OPSEC inspection checklists to sanitize facilities within their area of responsibility upon notification of an impending Chemical Warfare Convention (CWC), Strategic Arms Reduction Treaty (START) or Open Sky inspection. Group OPSEC managers, in consultation with their OPSEC monitors and unit security managers, shall specify on their checklist which items require shrouding consistent with security classification guides, Wing Items of Critical Information, input from personnel with technical knowledge of the area, equipment, hardware, etc.

3.4. A Wing OPSEC Working Group is established to ensure a viable, aggressive, and effective OPSEC program with continuity and direction. Membership of the OPSEC Working Group will be primary Group OPSEC managers, AFOSI Detachment 434, representatives from the security disciplines, contractor OPSEC focal points, intelligence officers, and others who play an integral role in maintaining effectiveness of the Wing mission. The Wing OPSEC Manager will convene the working group as necessary to help formulate OPSEC policy, establish procedures, develop survey scenarios, and address special concerns and tasking.

PAUL R. KLOCK, GS-14
Chief of Plans, XPR

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFPD 10-11, ***Operations Security***

AFI 10-1101, ***Operations Security (OPSEC) Instructions***

Abbreviations and Acronyms

CWC—Chemical Warfare Convention

OPSEC—Operations Security

START—Strategic Arms Reduction Treaty

SUI—Sensitive Unclassified Information

Terms

Adversary—An individual, group, organization or business competitor that must be denied critical and sensitive unclassified information.

Items of Critical Information—Pieces of information, generally unclassified, but when combined with other pieces of information, allows an adversary or competitor to draw conclusions about an organization's intentions, capabilities, vulnerabilities and limitations.

Operations Security (OPSEC)—The process of denying an adversary undisclosed information about the capabilities and intentions of Vandenberg AFB by identifying, controlling, and protecting items of critical and sensitive information associated with the planning and conduct of Wing operations.

OPSEC Vulnerability—A condition in which classified or sensitive unclassified information is subject to exploitation by an adversary.

OPSEC Countermeasure—Anything which effectively negates an adversary's ability to exploit an OPSEC vulnerability.

OPSEC Threat—The technical and operational capability of an adversary to detect and exploit vulnerabilities.

Sensitive Unclassified Information (SUI)—Information which does not meet security classification criteria, but could adversely affect U.S. national interests or the mission of the 30 SW if acquired by an adversary. The term includes records of information requiring protection under the Privacy Act, Freedom of Information Act, information designated "For Official Use Only," and items with limited distribution statements.