

**BY ORDER OF THE  
COMMANDER AIR MOBILITY COMMAND**



**AMC INSTRUCTION 10-704**

**1 JULY 1997**

**Operations**

**INFORMATION OPERATIONS**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** A copy of this publication can be found digitally at <http://www.safb.af.mil:80/hqamc/pa/pubs/pubhome2.htm>. If you lack access, contact your Publishing Distribution Office (PDO).

---

OPR: HQ AMC/DOKI (Major Michael S.  
DeJonge)

Certified by: HQ AMC/DOK (Lt Col Haren)  
Pages: 18  
Distribution: F

---

This instruction implements AFPD 10-7, *Command and Control Warfare*, and prescribes guidelines for the AMC Information Operations (IO) Program. It assigns responsibility for managing the AMC IO program. This instruction applies to AMC-gained United States Air Force Reserve units and Air National Guard units when published in the ANGIND 2. The reporting requirements in this directive are exempt from licensing in accordance with paragraph 2.11.10 of AFI 37-124, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections*.

## Chapter 1

### INFORMATION OPERATIONS CONCEPT

#### 1.1. Concept:

1.1.1. Definition of Information Operations (IO). Actions taken to affect adversary information and information systems while defending one's own information and information systems. (DoD Dir. 3600.1). The goal is to achieve an information advantage. IO can make a decisive difference at the strategic level by neutralizing an adversary's will and capacity to fight. IO can also facilitate military efforts at the operational and tactical levels by enabling freedom of action, security, initiative, and flexibility. Counterinformation and information assurance comprise the majority of IO efforts.

1.1.2. Information Operations Threat. Operation DESERT STORM marked a significant shift toward establishing information superiority. Coalition forces concentrated on establishing this control by attacking the adversary's C2 to deny the adversary the ability to coordinate forces. The emergence of a strategy to dominate information functions across the strategic, operational, and tactical spectrum throughout the entire conflict was key to coalition forces' combat dominance. However, information age warfare is more than technology, it requires new employment and organizational concepts. One of a commander's primary tasks is to gain and maintain information dominance with the objective of achieving faster and more effective command and control. IO is an enabling approach for organizing, training, equipping, and employing air and space power in the information age.

1.1.3. AMC Mission Statement. To direct, coordinate and participate in IO-related activities in support of the AMC mission. The AMC IO mission is both offensive and defensive. It includes defensive IO, offensive IO, and threat identification.

1.1.3.1. Defensive Information Operations. Composed of the following disciplines: Information Protection (IP), Information Security (INFOSEC), Psychological Operations (PSYOP), Military Deception, Counterintelligence Investigations, Intrusion Investigations, Intrusion Analysis, and Defensive Electronic Warfare (EW)

1.1.3.2. Offensive IO Operations. Composed of the following disciplines: Psychological Operations (PSYOP), Counterespionage Operations, Military Deception, Electronic Warfare (EW), and Physical Attack.

1.1.3.3. IO Threat Identification. Composed of the following disciplines: Acquisition Threat Assessments, Non-Government Agencies, Country Threats, System-Keyed Vulnerabilities, and Counterintelligence Collections.

#### 1.1.4. Key Aspects of Information Operations:

1.1.4.1. Electronic Warfare. Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack an adversary.

1.1.4.2. Information Attack. Encompasses special communications and computer activities taken to manipulate or destroy an adversary's information functions. An example might be interjection into a radar data stream causing fired anti-aircraft missiles to miss by a wide margin (e.g., 1000 feet).

1.1.4.3. Information Warfare. Those information operations employed in a crises or conflict are information warfare. Information warfare is to information operations what air combat is to air operations.

1.1.4.4. Military Deception. Actions executed to mislead foreign decision makers, causing them to derive and accept desired appreciation of military capabilities, intentions, operations, or other activities that evoke foreign actions that contribute to the originator's objectives.

1.1.4.5. Physical Attack. Destroys information systems through the conversion of stored energy into destructive power. The coupling of Precision Guided Munitions (PGM) and advanced delivery platforms provide the required precision to accurately attack the adversary's C2.

1.1.4.6. Psychological Operations. Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, group, and individuals. The purpose of psychological operations is to induce or reinforce attitudes and behavior favorable to the originator's objectives. (JP1-02)

1.1.4.7. Security Measures. Includes programs designed to protect information against corruption, destruction, and exploitation. (OPSEC, INFOSEC, COMSEC, EMSEC, and COMPUSEC are part of security measures.)

1.1.4.8. Tactical Military Deception. Military deception planned and executed by and in support of operational commanders against the pertinent threat to result in opposing operational actions favorable to the originator's plans and operations.

## Chapter 2

### HEADQUARTERS AND NAF RESPONSIBILITIES

#### 2.1. HQ AMC Responsibilities:

2.1.1. Command OPR for Information Operations. HQ AMC/DOKI will:

- 2.1.1.1. Ensure compliance with higher headquarters guidance, policy, and doctrine.
- 2.1.1.2. Ensure availability of IO training and education for HQ and unit-level personnel, through the Security Awareness, Training and Education (SATE) program.
- 2.1.1.3. Establish inspection criteria for assessment of unit-level IO programs.
- 2.1.1.4. Fund for or identify a process for funding IO-related activities.
- 2.1.1.5. Possess tasking authority over the Information Operations Working Group (IOWG) for IO-related issues.
- 2.1.1.6. Represent or ensure command representation at key IO-related meetings, user groups/forums, and provide feedback to HQ AMC IO points of contact.
- 2.1.1.7. Chair the HQ AMC IOWG. Use the IOWG to coordinate IO-related issues with each respective OPR.
- 2.1.1.8. Ensure AMC staff and units are advised on quickly changing IO-related policy, doctrine, and missions.
- 2.1.1.9. Periodically update AMC/CC and staff on IO-related issues. Advise AMC/CC and staff of IO issues facing the command.
- 2.1.1.10. Coordinate on all AMC IO requirements (i.e., Operational Requirements Documents, Mission Needs Statement, AMCIs, etc.).
- 2.1.1.11. Develop and track IO metrics for the command.

2.1.2. Integrated Functions. The following functions are integrated into the IO Branch.

- 2.1.2.1. Military Deception. Supplement higher headquarters guidance, policy, and doctrine. Provide oversight and deception experience.
  - 2.1.2.1.1. Plan, coordinate, and execute deception events.
  - 2.1.2.1.2. Develop deception annexes to OPLANS, CONPLAN, EXPLANS, and mobility plans.
  - 2.1.2.1.3. Implement, monitor, and evaluate deception awareness, education, and training programs.
- 2.1.2.2. Operations Security (OPSEC). Provide OPSEC expertise and management to the IO team.
  - 2.1.2.2.1. Integrate OPSEC into plans and directives.
  - 2.1.2.2.2. Coordinate training and education of OPSEC programs.

2.1.2.2.3. Identify MAJCOM critical information and indicators, and establish appropriate countermeasures.

2.1.2.3. Computers and Communication. Provides computer and communications expertise and management to the IO team. Acts as the conduit to SC for IO issues.

**2.1.3. Matrixed Functions.** The following functions are matrixed to the IO branch:

**2.1.3.1. AMC Information Protection (IP).** HQ AMC CPSS\STSP. Office provides:

2.1.3.1.1. Computer Security (COMPUSEC) expertise and management to the IO team.

2.1.3.1.1.1. Track accreditation status for all identified AMC Automated Information Systems (AIS).

2.1.3.1.1.2. Introduce security concerns early in development stage of new AMC systems.

2.1.3.1.1.3. Review formal incident reports from the Base IP offices and ensure the Air Force Information Warfare Center (AFIWC) is notified. Follow-up on reported incidents to ensure any vulnerabilities revealed are addressed and appropriate cross-feed information is distributed.

2.1.3.1.1.4. Assist in vulnerability assessments and recovery/repair efforts.

2.1.3.1.1.5. Retransmit Air Force Computer Emergency Response Team (AFCERT) advisories to alert personnel of suspected or actual vulnerabilities and their corresponding countermeasures.

2.1.3.1.2. Communications Security (COMSEC). COMSEC expertise and management to the IO team.

2.1.3.1.2.1. Evaluate all COMSEC incidents involving AMC material, personnel, or installations.

2.1.3.1.2.2. Monitor and evaluate all user COMSEC requirements for each AMC installation.

2.1.3.1.2.3. Evaluate requests for COMSEC material under AMC control.

2.1.3.1.2.4. Conduct biennial COMSEC functional reviews of each AMC COMSEC account.

2.1.3.1.2.5. Forward COMSEC review reports to the base COMSEC managers through their unit and wing/installation commanders.

2.1.3.1.2.6. Ensure follow-up actions are conducted on all command COMSEC reviews every 90 days or until corrected.

2.1.3.1.2.7. Ensure intertheater COMSEC Package (ICP) users under AMC COMSEC accounts receive current status, formulating policy, and doctrines on disseminating effective editions of COMSEC material.

2.1.3.1.3. Emission Security (EMSEC). EMSEC expertise and management to the IO team.

2.1.3.1.3.1. Review MAJCOM programming and requirements documents which call for the processing of classified information to ensure appropriate measures are taken to minimize and control emanations in accordance with national and DoD directives.

2.1.3.1.3.2. Provide EMSEC guidance and assistance to the command staff and subordinate wing IP offices on such matters as EMSEC assessments and countermeasures reviews.

2.1.3.1.4. Security Awareness Training and Education (SATE). Provide SATE expertise and management to the IO team.

2.1.3.1.4.1. Develop AMC-oriented Information Protection (IP) educational materials such as pamphlets, news articles, visual aids, films, and posters to support the command IP SATE program.

2.1.3.1.4.2. Train AMC personnel to assume responsibility for the protection of information generated, stored, processed, transferred, or communicated by Federal or Air Force automated systems.

2.1.3.2. Information Security. HQ AMC/SFI. Supports the AMC IO program by ensuring the proper protection and handling of classified material.

2.1.3.2.1. Provide training and guidance for Original Classification Authorities (OCAs), Top Secret Control Officers (TSCOs)/alternates, and security managers/alternates.

2.1.3.2.2. Provide guidance for protection of all levels of classified information.

2.1.3.2.3. Conduct physical security surveys of areas for open storage of classified material or other classified media and approval of discussion/conference rooms where classified information is used.

2.1.3.2.4. Conduct information security program reviews of AMC bases and HQ AMC activities when requested.

**2.1.3.3. Acquisition Threat Assessments.** HQ AMC/INO. Acquisition Threat Assessments OPR will support the IO office by assessing potential threats to systems in the acquisition cycle. INO analysts will, upon request, review the applicable threat portions of acquisition documentation and either validate or recommend changes as applicable. For substantive threat assessment taskings, INO will submit requests for support to the Defense Intelligence Agency and the Air Intelligence Agency. This requires sufficient lead time from requesters to ensure a quality response. IN will also support all IO related processes as required.

**2.1.3.4. Counterintelligence Support.** AFOSI. Air Force Office of Special Investigations (AFOSI) is the agency within the USAF chartered and authorized to conduct counterintelligence activities in support of Air Force commanders worldwide. Counterintelligence is defined as information gathering and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for, or on behalf of, foreign powers, organizations, persons, or international terrorist activities. AFOSI's support to IO can be defined in both offensive and defensive roles.

2.1.3.4.1. The offensive role includes the following:

**2.1.3.4.1.1. Counterespionage Operations.** That aspect of counterintelligence designed to detect, destroy, neutralize, exploit, or prevent espionage activities through identification, penetration, manipulation, deception, and respression of individuals, group, or organizations conducting or suspected of conducting espionage activities.

2.1.3.4.2. The defensive role includes the following:

**2.1.3.4.2.1. Counterintelligence Collections.** Collections focused on the timely and accurate production and dissemination of threat information relating to terrorists, foreign intelligence services, and criminal elements.

**2.1.3.4.2.2. Counterintelligence Investigations.** Investigations conducted to detect and neutralize foreign intelligence, terrorist, or subversive activities targeting USAF personnel, resources, and information.

**2.1.3.4.2.3. Intrusion Investigation and Analysis.** Investigations conducted by computer crime investigators and analysts on intrusions into USAF computer systems.

**2.1.3.4.3. 3d Field Investigations Region (3 FIR).** The primary mission of 3 FIR is to provide criminal investigative and counterintelligence support within Air Mobility Command (AMC) and Air Force Special Operations Command (AFSOC). As a member of the AMC IOWG, HQ 3 FIR/Office of Force Protection (FP) will advise HQ AMC/DOKI on counterintelligence issues (collection, investigation, or counterespionage-related matters). HQ 3 FIR/FP will also consult and coordinate with AFOSI computer crime investigators or computer crime analysts on intrusion matters.

**2.1.3.5. Electronic Warfare (EW).** HQ AMC/DOKT. Support the IO Branch by providing policy guidance, oversight, and electronic combat expertise to IO and command-related planning functions.

2.1.3.5.1. Develop EW annexes to OPLANS, CONPLANS, and other directives.

2.1.3.5.2. Identify and monitor EW awareness programs and initiatives.

2.1.3.5.3. AMC EW will evaluate applicability of supported commander EW recommendations.

2.1.3.6. Psychological Operations (PSYOP). HQ AMC/DOKJ. Support the IO branch by providing policy guidance, oversight, and PSYOP expertise to IO-related planning functions.

2.1.3.6.1. Develop PSYOP annexes to OPLANs, CONPLANs, and other directives.

2.1.3.6.2. Identify and monitor PSYOP awareness programs and initiatives.

2.1.3.6.3. Assist supported commander in delivery of PSYOP materials.

## **2.2. NAF Responsibilities:**

2.2.1. Each NAF/DO will establish a point of contact for IO within DO, SC, SF, and IN and pass to HQ AMC/DOKI for consolidation.

## Chapter 3

### UNIT LEVEL RESPONSIBILITIES

**3.1. Responsibilities.** This chapter contains minimum requirements for establishing and maintaining an IO program.

Each Wing, DRU, GSU, and AMC-gained Guard and Reserve Unit commander will:

- 3.1.1. Appoint in writing an O-3 or above with an operations background as the Information Operations Officer (IOO). Forward a copy of the appointment letter to HQ AMC/DOKI.
- 3.1.2. Notify HQ AMC/DOKI when IOO changes occur.

**3.2.** Each Unit IOO will:

- 3.2.1. Provide IO training inputs to the local OPSEC and SATE manager.
- 3.2.2. Operate and manage the IO program under the purview of the local commander and higher headquarters directives.
- 3.2.3. Establish an IOWG with members drawn from various support functions. Members will be identified in writing. The appointment letter will be kept in the unit IO continuity file.
- 3.2.4. Ensure the IOWG meets on a recurring basis, at least quarterly, or as contingencies or exercises require for effective mission coverage.
- 3.2.5. Provide IO program support and guidance to local commanders and agencies.
- 3.2.6. Conduct and evaluate local vulnerability assessments. Report adverse findings to local commanders as necessary.
- 3.2.7. Upchannel adverse IO trends or mission-critical IO findings to higher headquarters as they occur.
- 3.2.8. Request higher headquarters vulnerability assessments when deemed necessary by local commander.
- 3.2.9. Develop and maintain local supplements for higher headquarters' directives.
- 3.2.10. Develop, maintain, and forward appendices for OPLANs, exercises, and local operations to HQ AMC/DOKI for review and coordination.
- 3.2.11. Possess the proper security clearance for all IO related programs and insure IO working areas have the appropriate security protection.
- 3.2.12. Insure IO directives and training materials are current.

## Chapter 4

### AWARENESS, TRAINING, AND EDUCATION

**4.1. Awareness.** At a minimum, initial IO awareness training will include viewing the CYBER STRIKE training video series, reading the *Cornerstones of Information Operations* pamphlet from the CSAF, Air Force Doctrine Document 2.5, *Information Warfare* (Draft), and local procedures/guidance.

**4.2. Training/Education.** AMC's IO branch will disseminate IO-related materials through the AMC SATE program.

4.2.1. See AFCAT 36-2223, *USAF Formal Schools*, for a listing of IO-related training courses.

4.2.2. Unit IOOs will assign personnel to attend the Air University IO training course. HQ AMC/DOKI will secure and allocate quotas for the course as they become available.

GARY A. VOELLGER, Major General, USAF  
Director of Operations

## Attachment 1

### TERMS AND ACRONYMS

#### A1.1. Terms:

**A1.1.1. C2.** See command and control.

**A1.1.2. C2 Attack.** See command and control warfare.

**A1.1.3. Command and Control (C2) (DoD).** The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.

(Approved by JMTGM# 076-2864-94)

**A1.1.4. Command and Control Warfare (C2W).** The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare is an application of information warfare in military operations and is a subset of information warfare. Command and control warfare applies across the range of military operations and all levels of conflict. C2W is both offensive and defensive:

A1.1.4.1. C2-Attack--Prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system.

A1.1.4.2. C2-Protect—Maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system.

See also command and control; electronic warfare; intelligence; military deception; operations security; psychological operations.

(Approved by JMTGM# 034-96)

**A1.1.5. Communications Security (COMSEC) (DoD).** The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Communications security includes: cryptosecurity, transmission security, emission security, and physical security of communications security materials and information.

A1.1.5.1. Cryptosecurity--The component of communications security that results from the provision of technically sound cryptosystems and their proper use.

A1.1.5.2. Transmission Security--The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

A1.1.5.3. Emission Security--The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems.

A1.1.5.4. Physical Security--The component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons.

(JP 1-02)

**A1.1.6. Computer Security (COMPUSEC) (DoD).** The protector resulting from all measures to deny unauthorized access and exploitation of friendly computer systems. See also communication security. (Approved by JMTGM# -086-96)

**A1.1.7. Counter Information.** Seeks to establish a desired degree of information superiority by the destruction or neutralization of enemy offensive information operations.

**A1.1.8. Counterintelligence (CI) (DoD).** Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. See also counterespionage; countersabotage; countersubversion; security; security intelligence.

(JP 1-02)

**A1.1.9. Electronic Warfare (EW) (DoD).** Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW. The three major subdivisions within electronic warfare are, electronic attack, electronic protection, and electronic warfare support:

A1.1.9.1. Electronic Attack (EA)--That division of electronic warfare involving the use of electromagnetic, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. EA includes;

A1.1.9.1.1. Actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and

A1.1.9.1.2. Employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams)

A1.1.9.2. Electronic Protection (EP)--That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability.

A1.1.9.3. Electronic Warfare Support (ES)--That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support provides information required for immediate decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Electronic warfare support data can be used to produce signals intelligence, both communications intelligence, and electronics intelligence. See also command and control warfare; communications intelligence; directed energy;

directed-energy device; directed-energy warfare; directed-energy weapon; electromagnetic compatibility; electromagnetic deception; electromagnetic hardening; electromagnetic jamming; electromagnetic spectrum; electronics intelligence; frequency deconfliction; signals intelligence; spectrum management; suppression of enemy air defenses.

(Approved by JMTGM# 034-96)

**A1.1.10. Emission Security (EMSEC).** Protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto equipment, AIS, and telecommunications systems.

**A1.1.11. Information (DoD).**

A1.1.11.1. Facts, data, or instructions in any medium or form.

A1.1.11.2. The meaning that a human assigns to data by means of the known conventions used in their representation.

(Approved by JMTGM# 034-96)

**A1.1.12. Information Attack.** Directly corrupting information without visibly changing the physical entity within which it resides.

**A1.1.13. Information Operations (IO).** Actions taken to affect adversary information and information systems while defending one's own information, and information systems. (DoD Dir. 3600.1).

**A1.1.14. Information Operations Working Group (IOWG).** Composed of individuals from Tactical Deception, Information Protection, C4, OSI, Intelligence, Electronic Warfare, Military Deception, and Information Security, chaired by the IOO and brought together at least quarterly to work IO issues.

**A1.1.15. Information Protection (IP).** Composed of the following disciplines: Communications Security (COMSEC), Emissions Security (EMSEC), Computer Security (COMPUSEC), Operations Security (OPSEC), Physical Attack (PA), and Security Awareness Training and Education (SATE).

**A1.1.16. Information Security (INFOSEC).** The technical protection of information by Communications Security (COMSEC) and Computer Security (COMPUSEC) programs and protection of classified or sensitive information not covered by the COMSEC or COMPUSEC program.

**A1.1.17. Information Superiority (DoD).** That degree of dominance in the information domain which permits the conduct of operations without effective opposition. See also information.

(Approved by JMTGM# 034-96)

**A1.1.18. Intrusion Investigation and Analysis.** Investigations conducted by computer crime investigators and analysts on intrusions into USAF computer systems.

**A1.1.19. Military Deception (DoD).** Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. The five categories of military deception are:

A1.1.19.1. Strategic Military Deception--Military deception planned and executed by and in support of senior military commanders to result in adversary military policies and actions that support the originator's strategic military objectives, policies, and operations.

A1.1.19.2. Operational Military Deception--Military deception planned and executed by and in support of operational-level commanders to result in adversary actions that are favorable to the originator's objectives and operations. Operational military deception is planned and conducted in a theater of war to support campaigns and major operations.

A1.1.19.3. Tactical Military Deception--Military deception planned and executed by and in support of tactical commanders to result in adversary actions that are favorable to the originator's objectives and operations. Tactical military deception is planned and conducted to support battles and engagements.

A1.1.19.4. Service Military Deception--Military deception planned and executed by the Services that pertain to Service support to joint operations. Service military deception is designed to protect and enhance the combat capabilities of Service forces and systems.

A1.1.19.5. Military Deception in support of Operations Security (OPSEC)--Military deception planned and executed by and in support of all levels of command to support the prevention of the inadvertent compromise of sensitive or classified activities, capabilities, or intentions. Deceptive OPSEC measures are designed to distract foreign intelligence away from, or provide cover for, military operations and activities. See also deception.

(Approved by JMTGM# 055-2840-94)

**A1.1.20. Operations Security (OPSEC).** A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to identify those actions that can be observed by adversary intelligence systems, determine indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; or select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

**A1.1.21. Physical Attack.** The means by which targets are affected by hard weapons.

**A1.1.22. Psychological Operations (PSYOP).** Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, group, and individuals. The purpose of psychological operations is to induce or reinforce attitudes and behavior favorable to the originator's objectives. (JP1-02)

**A1.1.23. Security Awareness Training and Education (SATE).** A single, integrated security education, awareness, and training effort covering the communications security (COMSEC), computer security (COMPUSEC), and emissions security (EMSEC) disciplines. It is a training and indoctrination program established to emphasize C4 systems security awareness and to promote consistent application of security principles in the use of Air Force C4 systems.

**A1.1.24. Security Measures.** Includes all processes designed to protect information that could be corrupted, destroyed, or exploited across the range of military operations. This encompasses operations security (OPSEC) and Information Security (INFOSEC). OPSEC involves identifying critical information and subsequently analyzing friendly actions in order to preclude observation by adversary intelligence systems. INFOSEC relates to the technical protection of information by Communications Security (COMSEC) and Computer Security (COMPUSEC) programs.

## **A1.2. Acronyms.**

**ACC**—Air Combat Command  
**AETC**—Air Education and Training Command  
**AFCERT**—Air Force Computer Emergency Response Team  
**AFDD**—Air Force Doctrine Document  
**AFI**—Air Force Instruction  
**AFIWC**—Air Force Information Warfare Center  
**AFOSI**—Air Force Office of Special Investigations  
**AIA**—Air Intelligence Agency  
**AIS**—Automated Information System  
**AMC**—Air Mobility Command  
**AMCI**—Air Mobility Command Instruction  
**AMMP**—Air Mobility Master Plan  
**C2W**—Command and Control Warfare  
**C4**—Command, Control, Communications, and Computer  
**C&A**—Certification and Accreditation  
**CINC**—Commander in Chief  
**COMPUSEC**—Computer Security  
**COMSEC**—Communications Security  
**CONOPS**—Concept of Operations  
**DRU**—Direct Reporting Unit  
**EC**—Electronic Combat  
**EMSEC**—Emissions Security  
**EP**—Electronic Protection  
**ES**—Electronic Support  
**EW**—Electronic Warfare  
**HUMINT**—Human Intelligence  
**INFOSEC**—Information Security  
**IP**—Information Protection  
**IO**—Information Operations  
**IOWG**—Information Operations Working Group  
**JCS**—Joint Chiefs of Staff  
**MAJCOM**—Major Command

**OPLAN**—Operations Plan

**OPR**—Office of Primary Responsibility

**OPSEC**—Operations Security

**PSYOP**—Psychological Operations

**SATE**—Security Awareness, Training, and Education

**TACC**—Tanker Airlift Control Center

**Attachment 2****RELATED IO PUBLICATIONS****A2.1. Publications.**

Public Law 100-235, *The Computer Security Act of 1987*

CJCS MOP 6, *Electronic Warfare*

CJCS MOP 7, *Joint Strategic Planning System*

CJCS MOP 10, *Near Real-Time Analysis of Electromagnetic Interference and Jamming of US Space Systems*

CJCS MOP 24, *Tactical Employment of Directed-Energy Warfare Systems*

CJCS MOP 25, *Wartime Reserve Modes (WARM)*

CJCS MOP 29, *Joint Operations Security*

CJCS MOP 30, *Command and Control Warfare*

CJCS MOP 40, *Coordination of US C3 Positions in International Forums*

CJCS MOP 54, *Joint and Combined Communications Security Policy*

CJCS MOP 64, *Electromagnetic Spectrum Use in Joint Military Operations*

JCS MOP 116, *Military Deception*

DoDD 3222.3, *DoD Electromagnetic Compatibility Program*

DoDD 3222.4, *Electronic Warfare (EW) and Command, Control, Communications Countermeasures (C3CM)*

DoDD 3222.5, *Electromagnetic Compatibility (EMC) Management Program for SIGINT Sites*

DoDD 3321.1, *Overt Psychological Operations Conducted by the Military Services in Peacetime and in Contingencies Short of Declared War*

DoDD 3600.1, *Information Operations*

DoDD 4630.5, *Compatibility, Interoperability, and Integration of Command, Control, Communications and Intelligence Systems*

DoDI 4630.8, *Procedures for Compatibility, Interoperability, and Integration of C3I Systems*

DoDD 4650.1, *Management and Use of the Radio Frequency Spectrum*

DoD 5200.1, *Information Security Program*

DoD 5200.5, *Communications Security (COMSEC)*

DoDD 5205.2, *DoD Operations Security Program*

AFDD 2-5, *Information Warfare (Draft)*

AFPD 10-7, *Command and Control Warfare*

AFPD 10-11, *Operations Security (OPSEC)*

AFPD 31-4, *Information Security*

AFPD 33-2, *Information Protection*

AFPD 71-1, *Criminal Investigations and Counterintelligence*

AFI 10-701, *Performing Electronic Countermeasures in the United States and Canada (Draft)*

AFI 10-702, *Psychological Operations (PSYOP)*

AFI 10-703, *Electronic Warfare Integrated Reprogramming*

AFI 10-704, *Military Deception Program*

AFI 10-705, *(S) Command and Control Warfare Procedures (U)*

AFI 10-706, *Electronic Warfare (EW)*

AFI 10-707, *Spectrum Interference Resolution Program*

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

AFI 31-401, *Managing the Information Security Program*

AFI 33-201, *The Communications Security (COMSEC) Program (Draft)*

AFI 33-202, *The Computer Security (COMPUSEC) Program (Draft)*

AFI 33-203, *The Air Force Emission Security Program*

AFI 33-204, *The C4 Systems Security Awareness, Training, and Education (SATE) Program*

AFI 71-101, Volume I, *Criminal Investigations, Counterintelligence, and Protective Service Matters*

AFM 1-1, Volume I, *Basic Aerospace Doctrine of the United States Air Force*

**Attachment 3****10 PRACTICAL INFORMATION PROTECTION (IP) TIPS**

The following are a few tips to protect against an intrusion of your automated systems:

**A3.1.** Be careful about what you put in the trash can--shred old unit recall rosters, social security numbers, addresses, etc.

**A3.2.** Don't say anything over an unsecure telephone or send anything over unclassified E-mail systems that you wouldn't want to read in the newspaper.

**A3.3.** Lock your office, file cabinets, computers, and disk boxes when not in use; don't leave your floppy disks laying around.

**A3.4.** Don't leave your terminal/computer unattended when connected to another system (either via modem or local area network). Use a screen saver password; although this is far from secure, it will preclude casual snooping in your system.

**A3.5.** Avoid using common passwords (i.e., birthdays and nicknames). Change your password frequently, and BE UNPREDICTABLE!!! Insert special characters and numbers into your password, i.e., "5p1kefa\$t" instead of "spikefast."

**A3.6.** Never write your password down--memorize it.

**A3.7.** Virus check your system on a regular basis (i.e., weekly). Virus check any new software you receive electronically or on removable media, i.e., floppy disks or CD-ROM before using it in your computer.

**A3.8.** Periodically back up important files to tape or floppy disk and store them in separate locations.

**A3.9.** Use data encryption techniques whenever possible.

**A3.10.** Notify your system administrator of any unusual problems with your computer--unexplained data loss, slower operating speeds, or hardware malfunctions, etc.