BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-204

21 September 2001

Communications and Information

INFORMATION ASSURANCE (IA) AWARENESS PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

OPR: HQ AFCA/GCIS (MSgt Gary Sims)

Certified by: HQ USAF/SCXX (Mr. James J. Hundley)

Supersedes AFI 33-204, 26 April 1999.

Pages: 10
Distribution: F

This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-2, *Information Protection* (will become *Information Assurance* when publication is revised*)*, and applicable parts of National Institute for Standards and Technology (NIST) Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model,* April 1998; National Security Telecommunications and Information Systems Security Directive (NSTISSD) 500, (FOUO) *Information Systems Security (INFOSEC) Education, Training, and Awareness (U),* 25 February 1993; NSTISSD 501, (FOUO) *National Training Program for Information Systems Security (INFOSEC) Professionals (U),* 16 November 1992; Executive Order (EO) 12958, *Classified National Security Information*, April 17, 1995 (amended by EO 13142 dated November 19, 1999); Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources* (Appendix III, *Security of Federal Automated Information Resources*); Title 5 Code of Federal Regulations (CFR), Chapter 1, *Office of Personnel Management*, Part 930, *Programs for Specific Positions and Examinations (Miscellaneous)*; and the *Computer Security Act of 1987* (Public Law [P.L.] 100-235). It provides guidance and responsibility for establishing and managing the Information Assurance (IA) Awareness Program and defines program goals. This instruction applies to all Air Force military, civilians (to include volunteers and summer hires), and contractor personnel under contract by the Department of Defense (DoD), who use information systems. Additional security instructions and manuals are listed on the Air Force Publishing Web site at Uniform Resource Locator (URL): http://afpubs.hq.af.mil under Electronic Publications. Air Force Directory (AFDIR) 33-303, *Compendium of Communications and Information Terminology*, explains other terms. Direct questions or comments on the contents of this instruction, through appropriate command channels, to Headquarters Air Force Communications Agency (HQ AFCA/GCI), 203 W. Losey Street, Room 2200, Scott AFB IL 62225-5222. Refer recommended changes and conflicts between this and other publications to HQ AFCA/ITPP, 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, using AF Form 847, **Recommendation for Change of Publication**. See **Attachment 1** for a glossary of references and supporting information. Maintain and dispose of records created as a result of prescribed processes according to Air Force Manual (AFMAN) 37-139, *Records Disposition Schedule*

Report Documentation Page

Report Date 21 Sep 2001	**Report Type** N/A	**Dates Covered (from... to)** -

Title and Subtitle Air Force Instruction 33-204, Communications and Information Information Assurance (IA) Awareness Program	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Secretary of the Air Force Pentagon Washington, DC 20330-1250	**Performing Organization Report Number** AFI33-204
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor’s Acronym(s)**
	Sponsor/Monitor’s Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 10	

(will become AFMAN 33-322, Volume 4). The *Paperwork Reduction Act of 1980* (P.L. 96-511) and AFI 33-360, Volume 2, *Forms Management Program*, affect this publication.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

This revision changes the term "Security Awareness, Training, and Education (SATE) Program" to "Information Assurance Awareness Program" and updates the focus of this instruction. It deletes the requirement for training and education to be part of the awareness program and refers you to the applicable instructions for the training requirements. This update deletes the requirement for SATE biennial workshops, staff assistance visits, and major command (MAJCOM) or locally conducted workshops. It also deletes all references to reporting metrics and using the IA computer-based tutorial. The revision makes it mandatory for field operating agencies (FOA) and direct reporting units (DRU) to participate in their supporting host wing IA awareness program. It requires wing IA offices to ensure government contractors follow the provisions of this AFI when using government information systems. It adds responsibilities to the United States Air Force Academy (USAFA) and, due to organizational changes, the Deputy Chief of Staff/Communications and Information replaces the Air Force Communications and Information Center. The (|) preceding the publication title indicates a major revision from the previous edition.

Section A—General Information

1. Introduction . Information assurance (IA) is a key component of information operations (IO), used to achieve information superiority. This instruction describes and defines the IA Awareness Program goals, objectives, and standards. IA awareness is an integrated communications awareness program covering communications security (COMSEC), computer security (COMPUSEC), and emission security (EMSEC) disciplines. The program emphasizes IA principles and promotes consistent application of security principles during the use of Air Force information systems. ***NOTE:*** IA training and education is a requirement of assigned specialized duties and is separate from the IA Awareness Program. **Section D** identifies those specialized requirements.

2. Goal . The goal of IA awareness is to integrate information systems security policy and practices into the Air Force culture and minimize the opportunity for system compromise. Ensure all personnel using Air Force information systems understand the necessity and practice of safeguarding information processed, stored, or transmitted on all these systems. Personnel must understand various concepts of IA countermeasures to protect systems and information from sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or access by unauthorized persons.

3. Objectives . The objectives of the IA Awareness Program are to ensure individuals:

3.1. Understand the inherent weaknesses in information systems and the potential harm to national security due to the improper use of information systems.

3.2. Understand the existence of vulnerabilities and threats, and that Air Force information systems require protection from such vulnerabilities and threats.

3.3. Take necessary measures to protect information generated, stored, processed, transferred, or communicated by information systems.

3.4. Recognize practices and conditions that create vulnerabilities in information systems and use established procedures to mitigate them.

3.5. Recognize the potential damage to national security if COMSEC material is compromised and understand the security measures required in protecting this material.

3.6. Protect information systems and data against denial of service and unauthorized (accidental or intentional) disclosure, modification, or destruction.

3.7. Understand how COMPUSEC, COMSEC, and EMSEC relate to the overall protection of information generated, processed, stored, or transferred by information systems.

3.8. Implement practices to assure availability, integrity, authentication, confidentiality, and nonrepudiation are maintained to sustain the mission.

Section B—Roles and Responsibilities

4. Headquarters United States Air Force (HQ USAF) . The Deputy Chief of Staff/Communications and Information (HQ USAF/SC) is the Air Staff office of primary responsibility (OPR) for the Air Force Information Assurance Program.

5. Deputy Chief of Staff/Communications and Information, Information As surance Division (HQ USAF/SCMI):

5.1. Provides overall direction for the Air Force IA Program including the IA Awareness Program.

5.2. Works with HQ AFCA/GCI on all IA awareness and training issues.

6. Headquarters Air Force Communications Agency :

6.1. Provides oversight of the Air Force IA Awareness Program.

6.2. Guides, monitors, and assists MAJCOM IA offices as they implement their IA Awareness Program efforts.

6.3. Develops and publishes IA articles and generalized awareness materials, such as pamphlets, flyers, posters, trifolds, and videotapes, to support Air Force IA.

6.4. Serves as the OPR for IA awareness materials.

6.5. Reviews and approves developed IA awareness materials, including implementing documents submitted by Air Force personnel.

6.6. Works with HQ USAF/SCMI on IA awareness and training issues.

6.7. Serves as the subject matter expert for IA training and education materials. Provides advisory assistance for IA program development for all formal courses.

6.8. Administers the Air Force IA Home Page (https://www.afca.scott.af.mil/ip/) to disseminate and crossfeed IA information and promote IA awareness.

7. Headquarters Air Education and Training Command (HQ AETC) :

7.1. Conducts IA awareness training during initial military training (basic military training, Officer Training School, Air Force Reserve Officer Training Corps, and specialized training in Air Force Specialty Code [AFSC]-awarding courses).

7.2. Ensures all IA objectives outlined in paragraph **3.** are effectively covered.

7.3. Stresses that there is a point of contact (POC) for IA awareness in every Air Force unit and wing IA office.

7.4. Administers IA awareness training to students attending Air University courses.

7.5. Coordinates IA awareness materials with HQ AFCA/GCI.

7.6. Integrates IA education and training into the Air Force accession programs through AFSC-awarding courses, formal schools, and professional military education courses to:

7.6.1. Provide students with an understanding of IA and of the threat to, and vulnerabilities of Air Force information systems; a knowledge of countermeasures available to overcome the threat; and ways to apply the countermeasures.

7.6.2. Increase the depth of the formal training programs on the students' potential to become involved in planning, programming, managing, operating, or maintaining information systems.

7.6.3. Ensure courses address those aspects of IA that could affect the success of critical operations.

8. United States Air Force Academy :

8.1. Conducts IA awareness during initial military training.

8.2. Ensures all IA objectives outlined in paragraph **3.** are effectively covered.

8.3. Stresses that there is a POC for IA awareness in every Air Force unit and wing IA office.

8.4. Coordinates IA awareness materials with HQ AFCA/GCI.

9. Air Force Personnel Center (AFPC) . AFPC provides IA awareness for PALACE ACQUIRE-accessioned civilians through the civilian career programs.

10. Air Force Specialty Functional Managers . Deputy Chief of Staff/Communications and Information, Force Management Division (HQ USAF/SCXF) is the Air Force specialty functional manager for AFSC 3AXXX, Information Management; 3CXXX, Communications-Computer Systems; and 33SX, Communications-Information Systems.

10.1. Coordinates course development for IA training materials with HQ AFCA/GCI through the MAJCOM functional manager and MAJCOM IA office.

11. Major Command Information Assurance Offices :

11.1. Participate in the Air Force IA Awareness Program and support their wing IA awareness programs.

11.2. Develop command-oriented IA awareness materials such as pamphlets, news articles, and videotapes to support the command IA awareness program as needed. Provide all materials to subordinate units for use and to HQ AFCA/GCI for review and crossfeed.

11.3. Review the Air Force IA Web site pages monthly and incorporate IA materials into MAJCOM and wing IA awareness programs.

12. Air Force Field Operating Agencies and Direct Reporting Units :

12.1. Participate in supporting host wing's IA awareness program via the base Host Tenant Support Agreement.

12.2. Agencies and units not located on an installation will follow policy guidance in paragraphs **13.**, **14.**, and **15.**

13. Host Wing Commanders :

13.1. Ensure the host SC (or senior communications officer or commander) designates, in writing, primary and alternate individuals within the wing IA office to manage the wing IA awareness program.

13.2. Ensure these managers are knowledgeable about information systems security and operations.

14. Host Wing Information Assurance Offices :

14.1. Implement, manage, and conduct base-wide IA awareness programs. Make IA awareness information and materials available for all wing and tenant unit IA awareness managers and crossfeed locally developed materials among those unit managers and their MAJCOM.

14.2. Ensure IA awareness is available to all information system users, including all tenants, geographically separated units/isolated field offices, detachments, and remote operating locations.

14.3. Ensure government contractors follow the provisions of this instruction when using Air Force information systems in support of Air Force contracts to generate, process, store, transfer, or communicate information, as applicable.

14.4. Ensure unit IA awareness managers make maximum use of IA posters, pamphlets, screen savers, educational videotapes, and briefings, and emphasize use of these awareness tools.

14.5. Place reminders of the need for positive IA practices in base bulletins and other media to promote and reinforce IA awareness.

14.6. Maintain appointment letters of all unit IA awareness managers. Brief newly appointed host and tenant unit IA awareness managers on the IA awareness program.

14.7. Review the Air Force and MAJCOM IA Web site pages monthly and incorporate IA materials into the wing IA awareness program.

14.8. Ensure unit IA awareness managers are assessed and assisted as required by AFI 33-230, *Information Protection Assessment and Assistance Program*.

15. Unit Commanders :

15.1. Appoint a unit IA awareness manager and an alternate to manage the unit IA awareness program. Provide a copy of the appointment letter to the wing IA office. Recommend these duties be assigned to workgroup managers or information system security officers.

15.2. Review the unit IA awareness program and ensure compliance with IA awareness requirements.

16. Unit Information Assurance Awareness Managers :

16.1. Support and implement the wing IA awareness program and coordinate IA awareness materials with the host wing IA office as needed.

16.2. Disseminate IA materials received from the wing IA office and display awareness aids throughout the organization.

Section C—Awareness

17. Awareness . Make the awareness useful by addressing IA issues that directly affect users (i.e., password construction, Internet “do’s and don’ts”, etc.). Address consequences if policies and procedures are not followed. Ensure the IA awareness objectives identified in paragraph **3.** are met. IA awareness must be recurring, repetitive, and provided on a continuous basis.

17.1. Awareness Requirements. AFCA will develop and disseminate IA awareness materials with assistance from MAJCOMs and HQ USAF/SCMI.

17.2. Awareness Materials. The IA awareness managers satisfy awareness requirements by displaying IA-related awareness aids (e.g., posters, flyers, trifolds, etc.), videos, use public service announcements, or providing applicable articles from unit, base, and command publications to unit personnel. Use command-tailored, Air Force-purchased, or other awareness materials to reemphasize IA obligations. Managers will encourage the use of IA screen savers and take advantage of base television cable channels and the overseas Armed Forces Radio and Television Service to advance IA awareness. Additionally, publish monthly articles on IA. Awareness products are listed on the Air Force IA Home Page at URL: https://www.afca.scott.af.mil/ip/.

Section D—Training

18. General Requirements . Depending on assigned duties, all military, civilian, and contractor personnel (to include volunteers and summer hires) using Air Force information systems will require specialized IA training.

18.1. For COMSEC training requirements see AFKAG-1, (FOUO) *Air Force Communications Security (COMSEC) Operations*; AFI 33-211, *Communications Security (COMSEC) User Requirements*; and AFI 33-209, *Operational Instruction for the Secure Telephone Unit (STU-III) Type 1*.

18.2. For EMSEC training requirements see AFI 33-203, *Emission Security*.

18.3. For COMPUSEC training requirements see AFI 33-202, *Computer Security*.

18.4. For software licensing and management and anti-piracy training requirements see AFI 33-114, *Software Management*.

18.5. For licensing network users training requirements see AFI 33-115, Volume 2, *Licensing Network Users and Certifying Network Professionals*. Air Force personnel using other than Air Force systems are subject to the training requirements of the service or agency providing network service. If the providing service or agency does not have a program, Air Force personnel using DoD systems will complete the Air Force training. Additionally, foreign and local nationals requiring access to Air Force and other U.S. Government networks in the performance of their official duties are also subject to training. ***NOTE:*** The process to license users replaces the former initial SATE training requirements.

19. Information Collections, Records, and Forms .

19.1. Information Collections. No information collections are created by this publication.

19.2. Records. Maintain appointment letters, IA awareness materials, and other administrative records created as a result of these processes according to the appropriate 37 series tables in AFMAN 37-139 (will become AFMAN 33-322, Volume 4).

19.3. Forms (Adopted and Prescribed).

19.3.1. Adopted Forms. AF Form 847, **Recommendation for Change of Publication**.

19.3.2. Prescribed Forms. No forms are prescribed by this publication.

JOHN L. WOODWARD, JR., Lt General, USAF
DCS/Communications and Information

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Computer Security Act of 1987 (P.L 100-235)

Paperwork Reduction Act of 1980 (P.L. 96-511)

Title 5 CFR, Chapter 1, *Office of Personnel Management*, Part 930, *Programs for Specific Positions and Examinations (Miscellaneous)*

EO 12958, *Classified National Security Information*, April 17, 1995 (amended by EO 13142, November 19, 1999)

NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model,* April 1998

NSTISSD 500, (FOUO) *Information Systems Security (INFOSEC) Education, Training, and Awareness (U)*, 25 February 1993

NSTISSD 501, (FOUO) *National Training Program for Information Systems Security (INFOSEC) Professionals (U)*, 16 November 1992

OMB Circular A-130, *Management of Federal Information Resources* (Appendix III, *Security of Federal Automated Information Resources*)

AFPD 33-2, *Information Protection* (will become *Information Assurance* when publication is revised)

AFI 33-114, *Software Management*

AFI 33-115, Volume 2, *Licensing Network Users and Certifying Network Professionals*

AFI 33-202, *Computer Security*

AFI 33-203, *Emission Security*

AFI 33-209, *Operational Instruction for the Secure Telephone Unit (STU-III) Type 1*

AFI 33-211, *Communications Security (COMSEC) User Requirements*

AFI 33-230, *Information Protection Assessment and Assistance Program*

AFI 33-360, Volume 2, *Forms Management Program*

AFMAN 37-139, *Records Disposition Schedule* (will become AFMAN 33-322, Volume 4)

AFDIR 33-303, *Compendium of Communications and Information Terminology*

AFKAG-1, (FOUO) *Air Force Communications Security (COMSEC) Operations (U)*

Abbreviations and Acronyms

AFDIR—Air Force Directory

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFPC—Air Force Personnel Center

AFPD—Air Force Policy Directive

AFSC—Air Force Specialty Code

CFR—Code of Federal Regulations

COMPUSEC—Computer Security

COMSEC—Communications Security

DoD—Department of Defense

DRU—Direct Reporting Unit

EMSEC—Emission Security

EO—Executive Order

FOA—Field Operating Agency

FOUO—For Official Use Only

HQ AETC—Headquarters Air Education and Training Command

HQ AFCA—Headquarters Air Force Communications Agency

HQ USAF—Headquarters United States Air Force

IA—Information Assurance

INFOSEC—Information Security

IO—Information Operations

MAJCOM—Major Command

NIST—National Institute for Standards and Technology

NSTISSD—National Security Telecommunications and Information Systems Security Directive

OMB—Office of Management and Budget

OPR—Office of Primary Responsibility

P.L.—Public Law

POC—Point of Contact

SATE—Security Awareness, Training, and Education

STU—Secure Telephone Unit

URL—Uniform Resource Locator

USAFA—United States Air Force Academy

Terms

Communications Security (COMSEC)—Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such communications.

Computer Security (COMPUSEC)—Measures and controls that ensure the confidentiality, integrity, and availability of information systems assets including hardware, software, firmware, and information being processed, stored, and communicated.

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 cryptographic equipment, information systems, and telecommunications systems.

Information Assurance (IA)—Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Operations (IO)—Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Information Superiority—The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

Information System—Any telecommunications and/or computer-related equipment or interconnected system or subsystem of equipment that information systems use in the acquisition, storage, manipulation, management, movement, control, display, switching interchange, transmission, or reception, of voice and/or data, and includes software, firmware, and hardware. ***NOTE:*** This term replaces automated information systems (AIS).