***BY ORDER OF THE***
***AIR FORCE INSTRUCTION 33-200***

***SECRETARY OF THE AIR FORCE***

***23 DECEMBER 2008***

*Incorporating Change 1, 30 May 2009*
Certified Current 17 December 2009
***Communications and Information***

***INFORMATION ASSURANCE (IA) MANAGEMENT***

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

**ACCESSIBILITY:** Publications and forms are available on the e-Publishing website at **www.e-publishing.af.mil** for downloading or ordering.

**RELEASABILITY:** There are no releasability restrictions on this publication.

OPR: SAF/XCPP

Certified by: SAF/XCP-2
(Brig Gen Ronnie Hawkins)

Supersedes: AFI 33-202, Volume 1, 3 February 2006; AFI 33-204, 1 April 2004

Pages: 44

This Air Force Instruction (AFI) implements Air Force Policy Directive (AFPD) 33-2, Information Assurance (IA) Program, and establishes Air Force information assurance requirements for compliance with Public Law 100-235, Computer Security Act of 1987; Title 44 United States Code Section 3602; Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources; OMB Bulletin 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information; Title 10 United States Code (USC), Section 2224; Department of Defense Directive (DoDD) 8500.1, Information Assurance (IA); Department of Defense Instruction (DoDI) 8500.2, Information Assurance (IA) Implementation; DoDD 8100.2, Use of Commercial Wireless Devices, Services and Technologies in the Department of Defense (DoD) Global Information Grid; Chairman Joint Chiefs of Staff Instruction (CJCSI) 6510.01D, Information Assurance (IA) and Computer Network Defense (CND); and Chairman Joint Chiefs of Staff Manual (CJCSM) 6510.01, Defense-In-Depth: Information Assurance (IA) and Computer Network Defense (CND). This instruction provides the directive requirements for IA as outlined in AFPD 33-2. This instruction applies to all Air Force military, civilian, and contractor personnel under contract by DoD who develop, acquire, deliver, use, operate, or manage Air Force information systems (IS). This instruction applies to the Air National Guard and Air Force Reserve Command. The term major command (MAJCOM), when used in this publication, includes field operating agencies (FOA) and direct reporting units (DRU). Use of extracts from this instruction is encouraged. Committee on National Security Systems Instruction (CNSSI) No. 4009, National Information Assurance Glossary, explains other terms. Direct questions or comments on the contents of this instruction, through appropriate command channels, to Secretary of the Air Force, Policy and Resources Directorate (SAF/XCP), 1800 Air Force Pentagon, Suite 4C1059, Washington DC

20330-1800. Refer recommended changes and conflicts between this and other publications to HQ AFCA/EASD, 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, through appropriate channels, using Air Force IMT 847, Recommendation for Change of Publication. Provide an information copy to SAF/XCP. Send any supplements to this publication to SAF/XCP for review, coordination, and approval prior to publication. Provide a copy of each final supplement to HQ AFCA/EASD. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, Management of Records, and disposed of in accordance with Air Force Records Information Management System Records Disposition Schedule (RDS) located at **https://afrims.amc.af.mil/rds_series.cfm**. See Attachment 1 for a glossary of references and supporting information. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

***SUMMARY OF CHANGES***

This interim change modifies **paragraph 2.25.2.** to allow Wing IA Offices to achieve IA Certification Level I or II as opposed to only Level II. Air Force has coordinated this change with DoD NII and the change meets the intent of the requirement for local enclave certification requirements (Level I).

## Chapter 1

## GENERAL INFORMATION

**1.1. Introduction.** This AFI provides general direction for implementation of IA and management of IA programs according to AFPD 33-2. Compliance ensures appropriate measures are taken to ensure the availability, integrity, and confidentiality of Air Force ISs and the information they process. Using appropriate levels of protection against threats and vulnerabilities help prevent denial of service, corruption, compromise, fraud, waste, and abuse.

**1.2. Applicability.**

1.2.1. Applies to all ISs owned, operated, or supported by the Air Force, including IS components of weapon systems, ISs that provide the management infrastructure and connections among other ISs, and networks that are used to process, store, display, transmit or protect DoD information, regardless of classification or sensitivity. This document is also binding on all users that operate, connect, or interact with information systems owned, maintained, and controlled by the DoD.

1.2.2. More restrictive DoD and Intelligence Community directive requirements governing systems under the purview of the Intelligence Community take precedence over this instruction. For Sensitive Compartmented Information (SCI) systems, refer to Intelligence Community Directive (ICD) 503 and other Intelligence Community directives.

1.2.3. More detailed implementation guidelines are contained in IA reference documents and specialized publications cited throughout this AFI.

**1.3. Objectives.** Adequate security of Air Force information and supporting information technology (IT) assets is a fundamental management responsibility. The Air Force implements and maintains the IA Program to adequately secure its information and IT assets. The objectives, listed below, will be met through the effective employment of the Air Force's core IA disciplines of Communications Security (COMSEC), Computer Security (COMPUSEC), and Emissions Security (EMSEC). The IA Program:

1.3.1. Ensures Air Force ISs operate securely by protecting and maintaining the confidentiality, integrity, and availability of IS resources and information processed throughout the system's life cycle.

1.3.2. Protects information commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification.

## Chapter 2

## ROLES AND RESPONSIBILITIES

**2.1. Under Secretary of the Air Force (SAF/US).**

2.1.1. Ensures all Air Force-owned or controlled space systems meet the system specific IA requirements according to DoDD 8581.1, *Information Assurance (IA) Policy for Space Systems Used by the Department of Defense*.

2.1.2. For all space acquisitions, ensures IA requirements are implemented in all phases of acquisitions according to the provisions in NSS 03-01, *Guidance for DoD Space Systems Acquisition Process*.

**2.2. Assistant Secretary of the Air Force (Acquisition) (SAF/AQ).**

2.2.1. Ensures all IA requirements are implemented in all phases of non-space IS and service acquisitions, for research and development, test and evaluation, and in contracts.

2.2.2. Ensures Program Executive Officers (PEO) and Program Managers (PM) adhere to mandated IA acquisition standards outlined in DoDI 8580.1, *Information Assurance (IA) in the Defense Acquisition System*; the requirements of this instruction; and the certification and accreditation (C&A) requirements of AFI 33-210, *Certification and Accreditation (C&A) Program)*.

2.2.3. Ensures each program and system under its span of control develops an IA strategy according to this instruction and DoDI 8580.1.

2.2.4. Manages the process for preparing and reviewing Air Force acquisition program strategies and ensures IA has been appropriately addressed.

2.2.5. Represents the Air Force on policy and procedural matters regarding IA in the acquisition system.

2.2.6. Coordinates with USAF/A2 to ensure that Intelligence communications and information equipment, systems, and service acquisition efforts address IA life cycle requirements. Will coordinate with USAF/A2 to assign Air Force PM representatives for Intelligence systems, equipment, networks, or services that will deploy on the Air Force-provisioned portion of the Global Information Grid (AF-GIG) or will utilize AF GIG capabilities but which were developed and/or acquired by non-Air Force entities.

**2.3. Deputy Undersecretary of the Air Force, International Affairs (SAF/IA).** Processes all requests for transfers of COMSEC materials and associated information for foreign governments and international organizations.

**2.4. Secretary of the Air Force, Office of Warfighting Integration and Air Force Chief Information Officer (SAF/XC).** SAF/XC has the overall responsibility to develop, implement, and enforce policies, standards, strategies, and procedures to ensure the Air Force executes the most effective and efficient acquisition, integration, application, and management of information and IT assets. Further, as the Air Force Chief Information Officer, SAF/XC is the responsible official for Air Force owned and operated ISs.

2.4.1. Ensures IA is an integral part of ISs and applications design, guaranteeing appropriate IA controls are in place and provided to protect mission data and system resources.

2.4.2. Establishes the AF-GIG acceptable baseline risk level and IA controls.

2.4.3. Provides guidance, to implementing organizations, to mitigate threats commensurate with that risk level.

2.4.4. Provides guidance and solutions to organizations with operational requirements to meet the established national, DoD, Joint Chiefs of Staff, or Air Force baseline risk levels and controls for ISs.

2.4.5. Defines IA performance measures and metrics to identify enterprise-wide IA trends, to include IA related vulnerabilities and measures to mitigate them with an updated status of mitigation efforts using the program guidance in AFI 33-210.

2.4.6. Appoints the Designated Accrediting Authority (DAA) for the AF-GIG (AF-DAA) to execute specific responsibilities as outlined in AFI 33-210.

2.4.7. Review Internet Waiver/User Enclave Waiver requests for compliance to DOD GIG policy, DISN capability, and technical security requirements.

**2.5. Secretary of the Air Force, Policy and Resources Directorate (SAF/XCP).** SAF/XCP is the Air Force focal point to create an integrated, secure, net-centric environment to enable all aspects of the Air Force mission.

2.5.1. Develops, implements, and oversees an Air Force IA program focused on assurance of Air Force-specific information and ISs consistent with DoD policies and defense-in-depth.

2.5.2. Directs the establishment of IA policies and procedures. Informs Air Force secretariat, Headquarters Air Force, and MAJCOMs about changes to DoD and Air Force IA management policies and procedures.

2.5.3. Oversees IA requirements planning, programming, budgeting, and execution in the Air Force budget process and advocates for IA funding and manning with the Office of the Secretary of Defense and Congress.

2.5.4. Documents required IA capabilities in the Warfighter, Agile Combat Support, and ConstellationNet sub-enterprise architectures. Ensures IA capabilities are appropriately federated across the Air Force enterprise architecture. Directs and supports HQ AFCA in developing the ConstellationNet IA domain architecture.

2.5.5. Develops concepts and establishes policy for integrated support and configuration management of IA equipment.

2.5.6. Plans, programs, funds, implements, manages, and supports logistically the COMSEC aspects of programs, including centralized record maintenance of COMSEC equipment, components, and material.

2.5.7. Carries out FISMA-related Chief Information Officer (CIO) responsibilities and serves as SAF/XC's primary liaison to the Air Force's IA personnel.

2.5.7.1. Provides detailed information on the FISMA requirements via the annual Air Force FISMA Reporting Guidance.

2.5.7.2. Manages the annual assessment of Air Force IA Programs as required by FISMA. Requests, through channels, support from Air Force organizations. The support will allow Secretary of the Air Force/Policy and Resources (SAF/XCP-2) to answer the annual FISMA report questions posed by the Office of Management and Budget.

2.5.7.3. Collects and reports IA management, financial, and readiness data to meet DoD IA internal and external reporting requirements.

2.5.7.4. Ensures IA requirements are addressed and visible in all investment portfolios and investment programs according to AFI 33-401, *Implementing Air Force Architectures*, and AFI 33-210.

2.5.8. Manages the IA education, training, and certification for Air Force IA professionals and users according to DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, *Air Force Information Assurance Certification Implementation Plan*.

2.5.8.1. Defines and promulgates IA education, training, and certification standards.

2.5.8.2. Establishes timelines IA professionals must maintain to meet DoD and Air Force standards.

2.5.8.3. Ensures the education, training, and certification of Air Force IA professionals and the awareness and training of Air Force IT users according to paragraph 3.38.

2.5.9. Ensures personnel security is an integral part of the overall Air Force IA program and that personnel assigned to IA duties meet established personnel security requirements in AFI 31-501, *Personnel Security Program Management*.

2.5.10. Represents the Air Force as voting member on DoD Configuration Control Boards (CCB) or related to IA programs or issues (i.e., DoD Ports, Protocols, and Services [PPS] CCB).

2.5.11. Provides Air Force representation on DoD working groups on or related to IA programs or issues.

2.5.12. Coordinates with the other military departments and government agencies to eliminate duplication and to exchange technical data on IA programs.

2.5.13. Appoints in writing the Air Force Certified TEMPEST Technical Authority (CTTA).

2.5.14. Provides Air Force representation to DoD Information Assurance Technology Analysis Center, a formally chartered DoD institution that helps researchers, engineers, and program managers locate, analyze, use, and exchange scientific and technical information according to DoDD 3200.12, *DoD Scientific and Technical Information (STI) Program (STIP)*.

**2.6. Deputy Chief of Staff, Intelligence, Surveillance, and Reconnaissance (USAF/A2).** Manages, integrates and implements all IA capabilities for all SCI ISs and all ISs within SCI facilities.

**2.7. Office of the Air Force Civil Engineer (HQ USAF/A7C).** Serves as the Air Force focal point for design and construction of facilities containing radio frequency interference and electromagnetic interference shielding.

**2.8. Headquarters Air Education and Training Command (HQ AETC).**

2.8.1. Conducts and integrates IA education and training into initial military training courses, Air Force accession programs, formal schools, professional military education courses, and specialized training in Air Force Specialty Code-awarding courses according to AFI 36-2201V1, *Training Development, Delivery, and Evaluation*, and the specific IA education and training requirements of DoD 8570.01-M.

2.8.1.1. Provides students with:

2.8.1.1.1. An understanding of IA and of the threat to and vulnerabilities of Air Force ISs.

2.8.1.1.2. Knowledge of countermeasures available to overcome the threat.

2.8.1.1.3. Ways to apply the countermeasures.

2.8.1.2. Increases the depth of the formal training programs to enhance students' potential to become involved in planning, programming, managing, operating, or maintaining information systems.

2.8.1.3. Ensures courses address those aspects of IA that could affect the success of critical operations.

2.8.2. Administers IA education to students attending Air University courses.

2.8.3. Coordinates IA education materials and course curriculum with HQ AFCA to ensure they are current and meet the needs of a modern Air Force IA workforce.

**2.9. Headquarters Air Force Materiel Command (HQ AFMC).**

2.9.1. Supports PEOs and PMs in the research, development, prototyping, test and evaluation, assessment, production, and sustainment of IA or IA-enabled capabilities of non-space Air Force systems, products, and techniques in consultation with the other MAJCOMs.

2.9.1.1. Develops and sustains processes for rapid IA capability insertion to address new or rapidly developing threats to the AF-GIG.

2.9.1.2. Conducts the Air Force Communications-Computer Systems Security Research, Development, Test, and Evaluation Program according to AFI 63-101, *Operations of Capabilities Based Acquisition System*.

2.9.2. Ensures non-space PEOs and PMs comply with IA requirements outlined in DoDI 8580.1, AFI 63-101, this instruction, and AFI 33-210.

2.9.3. Ensures advanced development programs are reviewed for interoperability with IA equipment and systems.

2.9.4. Assists HQ AFCA in developing IA guidance and procedures for non-space ISs in the acquisition and development life cycle.

2.9.5. Establishes IA education and training for assigned PEOs and PMs according to the requirements outlined in DoD 8570.01-M.

2.9.6. Sustains a Public Key Infrastructure (PKI) program office to implement the Air Force portion of the DoD PKI and execute the designated responsibilities in AFI 33-202. Volume 6, *Identity Management* (will become AFSSI 8520, *Identity Management)*.

2.9.7. Sustains a Cryptographic Modernization program office to implement the Air Force portion of NSA's COMSEC program and execute the designated responsibilities in AFSSI 4000-series publications.

2.9.8. Ensures IA-related configuration control information under its inventory control is available to the operations, maintenance, and logistics support organizations to maintain the integrity of countermeasures during an IS's life cycle.

2.9.9. Establishes configuration control procedures to ensure the continuity and integrity of countermeasures for information technology processing national security information under its inventory management.

2.9.10. Ensures technical analyses, cost estimates, and modification proposals for information systems that process national security information consider TEMPEST design and installation requirements. Refer to: National Security Telecommunications and Information Systems Security Advisory Memorandum TEMPEST/2-95, *Red/Black Installation Guidance*, and AFSSI 7700, *Emissions Security*.

2.9.11. Cryptologic Systems Group (CPSG). Provides technical and PM support to IA Lead Command programs, projects, and initiatives according to Air Force IA specialized publications.

**2.10. Headquarters Air Force Space Command (HQ AFSPC).**

2.10.1. Supports PEOs and PMs in the research, development, test and evaluation, and sustainment of IA or IA-enabled capabilities of Air Force space systems and products in consultation with the other MAJCOMs. This includes developing and sustaining processes for rapid IA capability insertion to address new or rapidly developing threats to the AF-GIG.

2.10.2. Ensures space PEOs and PMs comply with IA requirements outlined in DoDI 8580.1, NSS 03-01, this instruction, and AFI 33-210.

2.10.3. Assists HQ AFCA in developing IA guidance and procedures for space ISs in the acquisition and development life cycle.

2.10.4. Establishes IA education and training for space PEOs and PMs according to the requirements outlined in DoD 8570.01-M.

2.10.5. Participates in Cross Domain Solutions (CDS) program for AFSPC space mission systems. Advocates issues for customers with AFCA. Attends CDS meetings and participates in activities as required.

2.10.6. Executes the EMSEC program for space mission systems and coordinates with the Air Force CTTA.

**2.11. Air Force Network Operations Commander (AFNetOps/CC).**

2.11.1. Directs Air Force Network Defense (NetD) in accordance with AFPD 10-7, *Information Operations*.

2.11.2. Executes duties as the AF-DAA according to AFPD 33-2 and AFI 33-210.

2.11.3. Serves as the single point of contact for processing and supporting Air Force IA-related intelligence requests from Air Force and DoD intelligence entities (e.g. threat

assessment against the GIG). Provides SAF/XC staff with courtesy copies of requests and responses for assessment of impact on the Air Force IA Program.

2.11.4. Identify Air Force network intelligence requirements to USAF/A2.

2.11.5. Coordinates with Joint and Defense-wide program offices to ensure interoperability of IA solutions across the GIG.

2.11.6. Directs Air Force enclave boundary defense activities, measures, and operations.

2.11.7. Serves as the single IA coordination point for Joint or Defense Programs with plan to deploy ISs to Air Force enclaves according to the responsibilities and procedures outlined in AFI 33-210.

2.11.8. Provides support to national, DoD, and Air Force level technical advisory groups (TAG) [i.e., DIACAP TAG, DoD PPS TAG, etc.], as requested by SAF/XC.

2.11.9. Issues time compliance technical orders and modification kits for IA and IA-enabled equipment and ISs processing national security information under its inventory management control and scheduled for modification.

**2.12. Air Force Network Operations Center (AFNOC).**

2.12.1. Conducts the Air Force portion of Network Defense (NetD) mission.

2.12.2. Employs mechanisms and procedures to monitor all Air Force ISs to detect, report, and document unauthorized activity (successful or unsuccessful).

2.12.3. Institutes appropriate NetD countermeasures or corrective actions. Countermeasures will be coordinated with the OPR of the appropriate policy.

**2.13. Air Force Information Operations Center (AFIOC).**

2.13.1. Serves as member of DoD TAGs, as requested by SAF/XC or HQ AFCA.

2.13.2. Provides information on threats, vulnerabilities, and countermeasures associated with IA.

2.13.3. Evaluates IA or IA-enabled products. Provides evaluation reports to HQ AFCA and applicable program management offices.

2.13.4. Develops Tactics, Techniques, and Procedures.

2.13.5. Provides EMSEC technical support according to the AFSSI 7000-series publications.

**2.14. Headquarters Air Force Communications Agency (HQ AFCA).** On behalf of SAF/XCP and the Senior IA Officer, as defined in AFPD 33-2:

2.14.1. Reviews, evaluates, and interprets national, federal, and DOD IA policy and doctrine. Makes recommendations on implementation of the policy and doctrine to SAF/XCPP.

2.14.2. Develops Air Force IA policies and procedures. Develops, coordinates, and maintains SAF/XC approved Air Force publications pertaining to IA.

2.14.3. Develops, coordinates, promulgates, and maintains Air Force (component-level) IA Controls applicable to ISs residing on or connecting to the AF-GIG, if required.

2.14.4. Provides guidance and support to MAJCOM and wing IA offices in developing, implementing, and managing their IA programs.

2.14.5. Provides guidance to acquisition managers to consider IA requirements early in the system life cycle according to AFI 63-101 and AFI 33-210.

2.14.6. Serves as a member on national, federal, and DoD TAGs as Air Force subject matter expert for IA or IA-related issues (i.e., DIACAP TAG, TEMPEST TAG, DoD PPS TAG, etc.)

2.14.7. Manages the process of assessing security features of government-produced and commercial-off-the-shelf (COTS) software and hardware subsystems, according to AFI 33-210.

2.14.8. Develops applicable IA techniques and procedures with Air Force-wide implications.

2.14.9. Processes requests for exceptions, deviations, or waivers to Air Force IA policy and instructions.

2.14.10. Serves as the Air Force Lead Command for the Air Force implementation of DoD IA programs, projects, and initiatives according to AFI 10-901, *Lead Operating Command—Communications and Information Systems Management*.

2.14.10.1. Develops the operational and maintenance concepts for all aspects of IA Lead Command programs, in coordination with participating and operating commands.

2.14.10.2. Identifies, prioritizes, and documents IA user requirements in conjunction with the MAJCOMs.

2.14.11. Manages the Air Force CDS program.

2.14.11.1. Advocates issues from customers with Air Staff and the CDS Secret Internet Protocol Router Network (SIPRNet) Connection Approval Office at Defense Information Systems Agency (DISA).

2.14.11.2. Attends CDS meetings and participates in activities as required.

2.14.11.3. Serves as the Air Force focal point for coalition networking issues specific to the Command, Control, Communications and Computers Infostructure, core e-mail, file sharing, print, collaboration tools, VTC, and web browsing capabilities. Coordinates with focal points of other functional communities (HAF/A2, etc.) on coalition networking issues for other infostructures (Intelligence, Surveillance and Reconnaissance, etc.).

2.14.12. Manages the Air Force PPS program. Advocates issues from customers with Air Staff and the DoD PPS Program Manager at DISA.

2.14.13. Manages and executes the IA Notice and Consent certification process for the Air Force according to the procedures within AFI 33-219, *Telecommunications Monitoring and Assessment Program* (Section C) (will become AFSSI 8561, *IA Notice and Consent*.

2.14.14. Executes funding provided by OSD to train and certify the Air Force IA workforce according to DoDD 8570.01 and DoD 8570.01-M.

2.14.15. Advocates and coordinates IA manpower requirements with operating and participating commands.

2.14.16. Maintains a list of recommended COTS products supporting IA and IA-enabled solutions using the Infostructure Technology Reference Model (i-TRM) process.

2.14.17. Ensures Air Force contracting guidance reflects national, federal, DoD, and Air Force IA policy and procedures.

2.14.18. Advises HQ AETC on IA education materials and course curriculum.

2.14.19. Executes the Air Force COMSEC program.

2.14.19.1. Manages COMSEC incident processing and analysis.

2.14.19.2. Manages Cryptographic Access Program. Includes development and promulgation of AFCOMSEC Form 9, *Cryptographic Access Certificate*.

2.14.19.3. Performs COMSEC responsibilities as mandated by the AFSSI 4000-series publications. This includes developing necessary forms:

2.14.19.3.1. AF Form 4167, *Two Person COMSEC Material Inventory*

2.14.19.3.2. AF Form 4168, *COMSEC Responsible Officer and User Training Checklist*

2.14.20. Executes the Air Force EMSEC program.

2.14.20.1. Acts as the Air Force CTTA.

2.14.20.2. Performs EMSEC responsibilities as mandated by the AFSSI 7000-series publications. This includes developing necessary forms to include AF Form 4170, *Emission Security Assessments/Emission Security Countermeasures Reviews*

2.14.21. Manages the Air Force Information Assurance Assessment and Assistance Program (IAAP) according to AFI 33-230 (will become AFSSI 8560, *Information Assurance Assessment and Assistance Program).*

2.14.22. Develops the ConstellationNet IA domain architecture, related IA service profiles, and implementation guidance.

**2.15. Air Force Office of Special Investigations (AFOSI).** To the extent authorized by statute, Executive Order, and regulation, provides (on a recurring basis) to SAF/XC, SAF/AQ, SAF/US, AFNetOps, and other appropriate organizations with the following:

2.15.1. Threat information,

2.15.2. Analysis of counterintelligence (CI) threats, and

2.15.3. Cyber-CI threat assessments concerning current and emerging threats to the AF-GIG for developing IA countermeasure capabilities in support of the Air Force IA Program and IS IA Program.

**2.16. Air Force Personnel Center (AFPC)** . Provides IA awareness and education for PALACE ACQUIRE-accessioned civilians through the civilian career programs according to the requirements outlined in DoD 8570.01-M.

**2.17. United States Air Force Academy.**

2.17.1. Conducts IA education during initial military training according to the requirements outlined in DoD 8570.01-M.

2.17.2. Coordinates IA education materials with HQ AFCA.

**2.18. Single Manager, Program Manager, or Project Manager.** Identifies, implements, and ensures full integration of IA into all phases of their acquisition, upgrade, or modification programs, including initial design, development, testing, fielding, operation, and sustainment. Reference AFI 63-101, *Operations of Capabilities Base Acquisition System* and AFI 33-210 for guidance.

**2.19. Other Agencies Acquiring or Developing Information Technology.** Assume single manager responsibilities when developing systems or software outside a program management office structure. Reference AFI AFI 63-101 and AFI 33-210 for guidance.

**2.20. Designated Accrediting Authority.** Reference AFI 33-210 for DAA appointment, assignment, delegation, training requirements, and key roles and responsibilities.

2.20.1. Manages and executes the Air Force IS IA Program according to this instruction and AFI 33-210.

2.20.2. Makes appropriate decisions to balance security requirements, mission, and resources against the defined or perceived threat.

2.20.3. Approves exceptions, deviations or, waivers to Air Force IA requirements according to this instruction and AFI 33-210 for ISs under their purview.

**2.21. Information System Owners (ISO).** Reference AFPD 33-2 and AFI 33-210 for ISO assignment, roles and responsibilities.

**2.22. System Level Information Assurance Manager (IAM).** (NOTE: For system-level IA program see AFI 33-210.

2.22.1. Develops an IS-level IA program that identifies:

2.22.1.1. IA Architecture, requirements, objectives, and policies.

2.22.1.2. Personnel.

2.22.1.3. Processes and procedures.

2.22.2. Receives training and certification to DoD baseline requirements at IA Technical Level II or III, as applicable. Completes and maintains required IA Workforce Management training according to *Air Force Implementation Plan For DoD 8570.01-M*.

2.22.3. Implements and maintains an IS-level IA program and documents the IA program through the Air Force C&A process in AFI 33-210.

**2.23. System Level Information Assurance Officer (IAO).** (NOTE: For system-level IA program see AFI 33-210. Assists the enclave or information system-level IAM in meeting the duties and responsibilities outlined in paragraph 2.23., above and:

2.23.1. Receives training and certification to DoD baseline requirements at IA Technical Level I or II, as applicable. Completes and maintains required IA Workforce Management training according to *Air Force Implementation Plan For DoD 8570.01-M*.

2.23.2. Ensures all users have the requisite security clearances and supervisory need-to-know authorization, and are aware of their IA responsibilities before being granted access to Air Force ISs according to AFSSI 8522, *Access to Information Systems*.

2.23.3. In coordination with the IAM, initiates protective or corrective measures when an IA incident or vulnerability is discovered according to AFI 33-138, *Enterprise Network Operations Notification and Tracking*.

2.23.4. Ensures IA and IA-enabled software, hardware, and firmware comply with appropriate security configuration guidelines as referenced in Chapter 3 of this instruction.

2.23.5. Ensures all IS IA-related documentation is current and accessible to properly authorized individuals.

2.23.6. Implements and enforces all Air Force IS IA policies and procedures, as defined by its security C&A documentation as prescribed by AFI 33-210.

**2.24. MAJCOM IA Office or Function.** Develops, implements, oversees, and maintains a MAJCOM IA program that identifies IA architecture, requirements, objectives and policies; personnel; and processes and procedures.

2.24.1. Designates an IAM (for organization-level IA program) to SAF/XCPP and AFCA. Individuals in this position must be US citizens.

2.24.2. Receives training and certification to DOD baseline requirements at IA Management Level III. Completes and maintains required IA Workforce Management training according to *Air Force Information Assurance Certification Implementation Plan* (will become AFSSI 8570). NOTE: If the individual is performing only COMSEC management duties, DoD 8570.01-M does not require the individual to be certified under this program.

2.24.3. Plans, organizes, implements, and controls MAJCOM COMSEC activities. Acts as the MAJCOM COMSEC office of primary responsibility. Executes roles and responsibilities in the AFSSI 4000-series publications.

2.24.4. Establishes COMPUSEC within the MAJCOM IA office and is the office of primary record for MAJCOM COMPUSEC. Executes roles and responsibilities in the AFSSI 8500-series publications.

2.24.5. Establishes EMSEC within the MAJCOM IA office and is the office of primary responsibility for MAJCOM EMSEC requirements. Executes roles and responsibilities in the AFSSI 7000-series publications.

2.24.6. Serves as a member of any appropriate Configuration Control Boards (CCB) or steering groups to address MAJCOM IA program issues.

2.24.7. Coordinates IAAP visits and associated responsibilities according to AFI 33-230 (will become AFSSI 8560).

2.24.8. Ensures proper identification of manpower and personnel assigned to IA functions. Ensure this information is entered and maintained in the appropriate Air Force personnel databases.

2.24.9. Maintain organizational e-mail account with an SMTP alias of <majcom>.ia@us.af.mil.

**2.25. Wing IA Office.** Develops, implements, oversees and maintains a wing IA program that identifies IA architecture, requirements, objectives and policies; personnel; and processes and procedures. **NOTE:** For bases with more than one wing, the designated host wing is responsible

to provide this function, unless otherwise indicated in an agreement (e.g. Memorandum of Understanding).

2.25.1. Designates an IAM (for organization-level IA program) to their MAJCOM IA office. Individuals in this position must be US citizens.

2.25.2. Receives training and certification to DOD baseline requirements at IA Management Level I or Level II for all assigned IA personnel. Completes and maintains required IA Workforce Management training according to *Air Force Information Assurance Certification Implementation Plan* (will become AFSSI 8570). NOTE: If the individual is performing only COMSEC management duties, DoD 8570.01-M does not require the individual to be certified under this program.

2.25.3. Manages the overall COMSEC posture of their installation. Appoints one primary and at least one alternate COMSEC manager to oversee the wing COMSEC program and to assist and advise them in COMSEC matters. The wing commander may delegate appointment authority to the unit commander of the supporting COMSEC account.

2.25.4. Establishes COMPUSEC in the host wing IA office. The IA office addresses all COMPUSEC requirements on the base, including those of tenant units (i.e., FOAs, DRUs, and other MAJCOM units) unless formal agreements exist.

2.25.5. Establishes EMSEC in the host wing IA office. The IA office addresses all EMSEC requirements on the base, including those of tenant units (i.e., FOAs, DRUs, and other MAJCOM units) unless there are other formal agreements.

2.25.6. Assists all base organizations and tenants in the development and management of their IA program.

2.25.7. Provides oversight and direction to IAOs (for organization-level IA programs) according to this instruction and specialized IA publications. Specific responsibilities include but are not limited to:

2.25.7.1. Ensures IAOs receive proper IA management training.

2.25.7.2. Ensures IAOs are aware of and follow IA policies and procedures.

2.25.7.3. Ensures IAOs review weekly alerts, bulletins, and advisories impacting the security of an organization's IA program.

2.25.8. Ensures security instructions, guidance, and standard operating procedures (SOP) are prepared, maintained, and implemented by each unit.

2.25.9. Monitors implementation of security guidance and directs appropriate actions to remedy security deficiencies.

2.25.10. Ensures IA inspections, tests, and reviews are coordinated.

2.25.11. Ensures all IA management review items are tracked and reported.

2.25.12. Develops reporting procedures.

2.25.12.1. Report security violations and incidents to the DAA and Air Force network operations activities according to AFI 33-138, *Enterprise Network Operations Notification and Tracking*.

2.25.12.2. Ensures incidents are properly reported to the DAA and the Air Force network operations reporting chain, as required, and that responses to IA-related alerts are coordinated; all according to the requirements of AFI 33-138.

2.25.13. Ensures procedures are developed and implemented according to configuration management (CM) policies and practices for authorizing use of software on ISs.

2.25.14. Serves as member of the base-level CM board or delegates this responsibility to an appropriate IAO.

2.25.15. Maintain organizational e-mail account with an SMTP alias of <wing>.ia@us.af.mil.

**2.26. Organizational Commander.** The organizational commander may locate his/her information assurance related roles and responsibilities in AFI 33-101, *Commanders Guidance and Responsibilities*.

**2.27. Organizational IAO.** IAOs are assigned to each organization by the organization commander or other cognizant authority (i.e., group-level commander, Wing IA office) when IA functions are consolidated to a central location or activity. Additional (subordinate) IAO positions may be assigned for additional support at the discretion of organizations or based upon mission requirements, however, only one primary and one alternate IAO is required. An organizational IAO:

2.27.1. Develops, implements, oversees, and maintains an organization IA program that identifies IA requirements, personnel, processes, and procedures.

2.27.2. Receives training and certification to DoD baseline requirements at IA Management Level I. Completes and maintains required IA Workforce Management training according to *Air Force Information Assurance Certification Implementation Plan* (will become AFSSI 8570).

2.27.3. Supervises the organization's IA program.

2.27.4. Implements and enforces all Air Force IA policies and procedures using the guidance within this instruction and applicable specialized IA publications.

2.27.5. Assists the wing IA office in meeting their duties and responsibilities.

2.27.6. Ensures all users have the requisite security clearances, supervisory need-to-know authorization, and are aware of their IA responsibilities (via IA training) before being granted access to Air Force ISs according to AFSSI 8522.

2.27.7. Ensures all users receive IA refresher training on an annual basis.

2.27.8. Ensures IT is operated, used, maintained, and disposed of properly and in accordance with the IT's security C&A documentation as prescribed by AFI 33-210.

2.27.9. Ensures proper CM procedures are followed. Prior to implementation and contingent upon necessary approval, according to this instruction and AFI 33-210, coordinates any changes or modifications to hardware, software, or firmware with the wing IA office and system-level IAM or IAO.

2.27.10. Reports IA incidents or vulnerabilities to the wing IA office.

2.27.11. In coordination with the wing IA office, initiates protective or corrective measures when an IA incident or vulnerability is discovered.

2.27.12. Implements required IA (COMSEC, COMPUSEC and EMSEC) countermeasures.

2.27.13. Maintains IA countermeasures.

2.27.14. Initiates requests for temporary and permanent exceptions, deviations, or waivers to IA requirements or criteria according to this instruction and applicable specialized IA publications.

2.27.15. Works with client support administrator(s) and unit security manager(s) in resolving classified message incidents.

**2.28. Information System Users.** Authorized users shall comply with the guidance within AFI 33-100, *User Responsibilities and Guidance For Information Systems*.

# Chapter 3

# POLICY

## *Section 3A—Air Force IA Program*

**3.1. Air Force IA Program.** The Air Force IA Program synchronizes and standardizes the IA requirements of Air Force ISs through the following means:

3.1.1. Integration of IA into all aspects of the Air Force Enterprise Architecture according to AFI 33-401.

3.1.2. Coordination of IA projects across multiple investments through Lead Command management according to AFI 10-901.

3.1.3. Improving the Air Force IT and National Security Systems (NSS) acquisition and fielding process through the IT Lean Process according to AFI 63-101 and AFI 33-210. Improvements are achieved in this streamlined process through appropriate oversight, standardized design and test, networthiness assessment, and fielding processes. The IT Lean Process aligns with the DIACAP required for all DoD-owned or controlled ISs that receive, process, store, display, or transmit DoD information. It does not alleviate the need to execute the DIACAP; however, the IT Lean Process and the integrated IA Controls in the Security, Interoperability, Supportability Sustainability, and Usability (SISSU) checklist can help the program team identify IA requirements. Refer to AFI 33-210 for complete policy and pointers to implementation procedures.

3.1.4. Clear assignment of Air Force organizational and IT level IA roles and responsibilities are outlined via this instruction and supporting IA specialized publications.

3.1.5. Development and management of a professional IA workforce according to the *Air Force Information Assurance Certification Implementation Plan* (will become AFSSI 8570).

**3.2. IA Strategy.** IA is traced, by SAF/XCP, as a programmatic entity in the Planning, Programming, Budgeting, and Execution system with visibility extended into budget execution. Air Force strategic IA goals and annual IA objectives are established (according to the DoD Information Management Strategic Plan). Funding and progress toward those objectives are tracked, reported, and validated through the Air Force IA Strategic Plan (upon approval of the plan).

**3.3. Air Force Specialized IA Publications.** These publications document implementation of Air Force IA policy objectives, under the authority of AFI 33-102, *Communications and Information Specialized Publications*. These publications are numbered based upon the primary subject groups cited below. Publication OPRs will regularly update or expand the content to keep pace with new threats and manage any challenges associated with introduction of emerging technologies.

3.3.1. AFSSI 3000 Series – COMSEC Equipment.

3.3.2. AFSSI 4000 Series – COMSEC Operations.

3.3.3. AFSSI 7000 Series – EMSEC.

3.3.4. AFSSI 8500 Series – IA Implementation.

3.3.5. As described in AFI 33-102, the unclassified specialized publications will be hosted on the Air Force IA website (**https://private.afca.af.mil/ip**). The For Official Use Only (FOUO) specialized publications will be hosted on the *Air Force IA Documentation (FOUO)* Community of Practice (CoP) (**https://afkm.wpafb.af.mil/ASPs/CoP/ClosedCOP.asp?Filter=OO-SC-CA-11H**). Classified specialized publications will be acquired from the office of primary responsibility.

**3.4. IA Workforce.** This instruction and supporting IA specialized publications standardize the naming conventions and functions of Air Force organizational (management) and IT level (technical or system-level) IA personnel. These documents also prescribe training and certification requirements according to national and DoD policy consistent with and supplementary to the guidance outlined in the *Air Force Information Assurance Certification Implementation Plan* (will become AFSSI 8570).

**3.5. IA Awareness.** All authorized users of Air Force IT must maintain an understanding of Air Force IA policies and procedures commensurate with their individual responsibilities. For a list of these and other user responsibilities, reference AFI 33-100.

**3.6. Network Defense (NetD).** Reference the below guidance for NetD:

3.6.1. AFPD 10-7, *Information Operations*, and subordinate AFIs govern Network Defense and INFOCON procedures.

3.6.2. AFPD 13-3, *Air Force Network Operations (AFNetOps)*, governs command and control of the AF-GIG.

**3.7. IA Assessments.** Designated Air Force (and DoD) activities will regularly and systematically assess the IA posture of Air Force networks and ISs as well as IA services and supporting infrastructures.

3.7.1. Auditors perform audits according to Air Force Audit Agency guidance.

3.7.2. Authorized activities perform host and network vulnerability or penetration testing according to guidance published by USAF/A3O-CN.

3.7.3. ISOs and PMs comply with formal testing and certification activities according to AFI 33-210.

3.7.4. Performance measures and metrics will assess enterprise-wide (and individual elements where appropriate) IA performance and assess IA trends. The measurements and metrics will encompass, but are not limited to, federal and DoD IA reporting requirements.

3.7.5. Information Assurance Assessment and Assistance Program. The IAAP is a staff function whose purpose is to ~~"~~find and fix" wing level IA problems. It is neither a function of, nor does it replace Inspector General or Air Force Audit Agency activities. The IAAP accomplishes ~~"~~staff assistance" by reviewing and assessing processes, identifying problems, providing assistance to help resolve the problems, and recommending solutions. The IAAP team provides technical and training assistance in all IA areas. The IAAP consists of two parts: assessment and assistance. IAAPs are performed according to AFI 33-230 (will become AFSSI 8560) through the review of areas itemized on AF Form 4160, *Information Assurance Assessment and Assistance Program (IAAP) Criteria*.

**3.8. Notice and Consent Certification.** All Air Force installations, circuits, and ISs must comply with DoD notice and consent certification requirements for monitoring to occur by

authorized activities. Comply with installation certification procedures found in AFI 33-219, (Section C) (will become AFSSI 8561).

**3.9. Connection Management.** SAF/XCD provides Air Force representation to the Defense Information Systems Network (DISN) Security Accreditation Working Group (DSAWG). The DSAWG represents the DISN community and advises the DISN DAAs of likely community acceptance or rejection of community risk. DISN connection decisions rest with the four DISN DAAs. SAF/XCD will work with Air Force activities involved in the adjudication of conflicts related to DISN connection decisions.

3.9.1. Air Force activities adhere to the DISA Connection Approval Process if the system is connected to the Non-Secure Internet Protocol Router Network (NIPRNet) or SIPRNet. Connection Approval Process information can be found at **http://iase.disa.mil/cap/index.html**. For all Air Force ISs accessing the DISN-SIPRNet, get appropriate service (e.g., DISA) coordination and authorization before proceeding with combatant command coordination and/or Joint Staff approval.

3.9.2. Air Force activities adhere to the guidance in AFI 33-210 for connection approval to the AF-GIG.

**3.10. Configuration Management.** The program manager (or designee) shall:

3.10.1. Review all changes to the configuration of IT (i.e., the introduction of new IT, changes in the capability of existing IT, changes to the infrastructure, procedural changes, or changes in the authorized or privileged user base, etc.) for IA impact prior to implementation.

3.10.2. Ensure interoperability and compatibility with existing Air Force standard IA policies and procedures according to the Air Force i-TRM (**https://itrm.hq.af.milH**).

**3.11. IA Products.** Reference AFI 33-210 for guidance on specified robustness of solutions and product specification and evaluation requirements. Check the Air Force Evaluated/Approved Products List (**https://afkm.wpafb.af.mil/IAH**) for recommended products and implementation guidance, respectively.

**3.12. Security Configuration and Implementation.** IA reference documents, such as National Institute of Standards and Technology Special Publications, DISA Security Technical Implementation Guides (STIG), and NSA Security Configuration Guides represent a collection of resources for the secure configuration, implementation and deployment of IA- and IA-enabled IT products that require use of the product's IA capabilities. Air Force specialized publications (AFSSIs, Air Force Technical Orders, etc.) may supplement these documents and provide Air Force specific implementation guidelines or guidance on the management of specific Air Force IA programs. Apply these IA documents to establish and maintain a minimum baseline security configuration and posture.

**3.13. Key Management Infrastructure (KMI).** The KMI provides a common unified process for the secure creation, distribution, and management of cryptographic products, such as asymmetric keys (e.g., PKI) and traditional symmetric keys (e.g., Electronic Key Management System) that enable security services for information systems. KMI-enabled services includes access control and identification and authentication.

3.13.1. PMs and IA professionals implement key management procedures according to AFI 33-202, Volume 6 (will become AFSSI 8520) for Public Key Infrastructure (PKI) and the appropriate AFSSI 3000- or 4000-series publication for specific cryptographic products.

3.13.2. PMs and IA professionals implement Identification and Authentication (I&A) using the DoD PKI Class 3 certificate and hardware security token, when available, according to AFI 33-202, Volume 6 (will become AFSSI 8520).

**3.14. Air Force IA Support Services.** AFCA supports the Air Force IA program through the maintenance of the Air Force IA website, *Air Force IA* CoPs, Air Force portion of DIACAP Knowledge Service, and traditional collaboration tools (i.e., electronic mail, the Air Force Portal, etc.) These resources provide immediate access and awareness to current Air Force, DoD and federal IA and IA-related policy and guidance, including recent and pending changes to Air Force policy and Air Force/DoD IA controls.

***Section 3B—Air Force Information System IA Program***

**3.15. Air Force Information System IA Program.** IAMs (enclave or system-level) are responsible for establishing, implementing, and maintaining the Air Force IS IA program.

3.15.1. IAMs will ensure their IS IA programs integrate with the Air Force IA Program using the Air Force C&A program AFI 33-210. Tracking and reporting management review items will be accomplished using the information registered in Enterprise Information Technology Data Repository (EITDR).

3.15.2. All elements of an Air Force IS IA program are developed, documented, implemented, and maintained through the Air Force C&A program. This program is the mechanism for coordinating IA requirements and capabilities between DoD and Air Force ISs, their supporting enclaves and the AF-GIG using a common baseline of standards referred to as IA Controls (see below). The Air Force C&A program includes guidance mandated by AFI 33-210 with implementation guidelines outlined by this instruction and specific procedure or program implementation through supporting specialized IA publications.

3.15.3. The IAM implements their IA program with the assistance of IAOs (system-level), as required, and other privileged users (network administrators, system administrators, database administrators, web administrators, etc.)

**3.16. IA Controls.** System designation, Mission Assurance Category (MAC) and confidentiality level (CL) establishment, as mandated by AFI 33-210, assist in the proper determination and management of IA requirements. These IA requirements are primarily expressed in the form of IA Controls. IA Controls, defined in detail within DoDI 8500.2, provide a common management language for establishing IA needs or conditions. These controls ensure systems are designed to meet those needs; implemented IA solutions are tested and validated; changes to the validated baseline are managed; interconnections to other ISs are coordinated; and provide a method for reporting IA readiness and posture. The baseline IA Controls for each of the combinations of MAC and CL are outlined within the enclosures to DoDI 8500.2.

3.16.1. PMs and/or IAMs identify and include DoD IA Controls in the design, acquisition, installation, operation, upgrade, or replacement of all Air Force ISs. DOD IA Controls

applicable to Air Force ISs must be addressed in all appropriate requirement documents. Additionally, DoD IA Controls are supplemented as follows:

3.16.1.1. The Air Force establishes IA Controls that apply to ISs residing on or connecting to the AF-GIG, if necessary. Air Force IA controls must be applied to Air Force ISs; Guest ISs (formerly known as Non-Air Force ISs; reference AFI 33-210 are not required to implement Air Force component IA controls. The Air Force IA Controls do not contradict nor negate DoD baseline IA Controls. They add to or supplement DoD IA Controls with Air Force specific requirements, implementation guidelines or fill gaps between national and DoD level IA requirements. At no time will Air Force IA Controls degrade interoperability across both the GIG and AF-GIG. As with DoD IA Controls, Air Force IA Controls are uniquely named and formally catalogued. EITDR provides the reference for these Air Force IA Controls and also serves as the vehicle for measuring and reporting compliance throughout the life cycle of an IS. Air Force instructions and specialized publications provide implementation guidelines for Air Force IA Controls. The first option is to propose the control to the DoD for inclusion in the baseline. If DoD declines to add them to the baseline, the Air Force may develop augmented controls according to the process in AFI 33-210.

3.16.1.2. Individual Air Force ISs may establish local, or augmented, IA Controls provided they are consistent with the paragraph above (3.16.1.1). Document these augmented controls through both the requirement and the C&A processes. If necessary, augmented controls provider a single system with additional protection from interconnected systems and address local threats or vulnerabilities. Local information system IA controls do not apply to other information systems and may not be used to deny connectivity of systems which meet baseline IA controls according to this instruction and AFI 33-210.

3.16.2. PMs and/or IAMs coordinate Automated Information System (AIS) application-unique requirements for Joint and Defense-wide programs through the Air Force Authority to Connect process according to AFI 33-210. Coordination must occur through this process for connections to the AF-GIG rather than with local Air Force enclaves.

**3.17. Information System Security Engineering (ISSE).** IA will be integrated into the overall system acquisition and engineering process throughout the entire system life cycle via the information system security engineering (ISSE), according to DoDI 8500.2.

**3.18. IT and IT Service Acquisitions.** IA will be implemented in all IT and services acquisitions (including space and non-space acquisitions) at levels appropriate to the system characteristics and requirements throughout the acquisition life cycle, according to AFI 63-101 and AFI 33-210.

**3.19. Communications Security.** COMSEC refers to measures and controls taken to deny unauthorized persons information derived from information systems of the United States Government related to national security and to ensure the authenticity of such ISs. COMSEC protection results from applying security measures (i.e., crypto security, transmission security, etc.) to communications and information systems generating, handling, storing, processing, or using classified or sensitive government or government-derived information, the loss of which could adversely affect the national security interest. It also includes applying physical security measures to COMSEC information or materials. Ensure all COMSEC activities comply with

AFI 33-201, Volume 1, (FOUO) Communications Security (COMSEC) (will become AFSSI 4201, (FOUO) *Communications Security* (COMSEC), and associated Air Force IA specialized publications.

**3.20. Computer Security for the Computing Environment.** Protect IT, its operating system, peripherals (media and devices), applications, and the information it contains against loss, misuse, unauthorized access, or modification. Ensure compliance with the standard procedures outlined in AFSSI 8502, *Computer Security*. These procedures ensure the computing environment complements the Air Force IS IA program. AFSSI 8502 does not present IA requirements and capabilities. These are achieved through the proper application of IA Controls for an information system. AFSSI 8502 provides standard procedures derived from IA Controls and other measures for organizations to maintain the confidentiality, integrity, and availability of any Air Force IS IA program.

**3.21. Emissions Security.** Deny interception and exploitation of classified, and in some instances unclassified, information by containing compromising emanations within an inspectable space. Implement measures to protect against compromising emanations according to AFSSI 7700 and associated EMSEC specialized publications.

**3.22. Identification and Authentication.**

3.22.1. Protect access to ISs commensurate with the sensitivity of the information the IS processes. Implement individual and group I&A procedures (i.e., tokens, logon IDs, passwords, PINs, etc.) according to AFMAN 33-223, *Identification and Authentication* (will become AFSSI 8520).

3.22.2. Ensure only authorized users maintain access to workstations, applications, and networks.

3.22.3. Implement a comprehensive account management process according to AFMAN 33-223, (will become AFSSI 8520)

**3.23. Access Control.**

3.23.1. Ensure only authorized users can gain access to workstations, applications, and networks. Grant access to information systems based on need-to-know, classification level of the information, security clearance, for official government business, special access (e.g., foreign national access), Information Technology [IT] (formerly Automated Information Systems [AIS]) category designated requirements (i.e., local background investigation, national agency check, etc.), and qualifications. Comply with the implementation procedures and approval guidelines in AFSSI 8522 prior to granting system access. This guidance also provides procedures for Foreign National access, access suspension and other access requirements.

3.23.2. Foreign National Access.

3.23.2.1. AFNetOps/CC approved access by foreign nationals to unclassified Air Force Information Systems (IS) where AFNetOps/CC is the Designated Accrediting Authority (DAA) or has delegated that responsibility. Before foreign nationals are authorized access and use of ISs, they must meet the requirements of AFI 31-501 and AFSSI 8522. This includes the AF provisioned portion of the Global Information Grid (GIG), (e.g. unclassified base LAN).

3.23.2.2. Access by foreign nationals to Air Force Information Systems where AFNetOps/CC is not the DAA (SAP/SAR and Space) requires approval by the lead DAA for these systems. Before foreign nationals are authorized access and use of SAP/SAR and Space system, they also must meet the requirements of AFI 31-501, AFSSI 8522 and applicable guidance for those information systems.

**3.24. Controlling Maintenance Activities.** Restrict IS maintenance to authorized personnel with a security clearance for the highest classification and most restricted category of information processed. Adhere to the requirements of AFSSI 8522 to develop processes for determining authorization and controlling access to information and resources.

**3.25. Network Security for the Enclave Environment.** The proper application of IA Controls through the C&A process establishes the IA requirements and capabilities for enclaves under the Air Force IS IA Program.

**3.26. Boundary Defense.** Deploy boundary defense mechanisms (i.e., firewalls, network intrusion detection systems, filtering services, etc.) at the Air Force enclave boundary to other enclaves and the wide area network; at layered or internal enclave boundaries; and at key points in the network, as required. Access to external, untrusted networks (i.e., public Internet, commercial wide area networks, Federal networks, etc.) is only permitted from a demilitarized zone (DMZ) in accordance with CJCSM 6510.01. Connections between Air Force enclaves and foreign (or coalition) networks also require a DMZ or CDS.

**3.27. Malicious Logic Protection.** Protect IT from malicious logic (i.e., virus, worm, Trojan horse, etc.) attacks. Apply an appropriate mix of preventive measures to include user awareness training, local policies, configuration management, and antivirus software according to the IA Controls for an Air Force IS IA Program and AFSSI 8502 for the computing environment.

**3.28. Incident Response and Reporting.** AFI 33-138 defines reportable incidents, outlines SOPs for incident response, outlines user requirements, and establishes requirements for incident response in the AFNetOps hierarchy. Refer to AFNetOps instructions and procedures for classified message incidents.

**3.29. Vulnerability Management.** Comply with AFI 33-138 for the vulnerability management process which includes systematic identification and mitigation of software and hardware vulnerabilities.

**3.30. Information Operations Condition.** The INFOCON system is a commander's alert system that establishes a uniform process for posturing and defending against malicious activity targeted against DoD ISs. The system provides a predefined sequence of actions necessary for achieving a common level of information security for DoD ISs. Comply with the requirements of AFI 10-710, *Information Operations Condition (INFOCON)*, for Air Force implementation of INFOCON requirements.

**3.31. Interconnections Among Systems and Enclaves.**

3.31.1. The only DoD authorized access to the Internet is via the NIPRNet. If an organization requires a connection to the Internet via a Commercial ISP submit a waiver request through SAF/XCD, as the Air Force representative to the DoD GIG Board. Use AF 4169, *Request for Waiver from Information Assurance Criteria*, to document the request. The waiver request shall explain how the non-NIPRNet Internet connections meet the

minimum security standards established by the DSAWG and be accompanied by a plan to transition the connection to the NIPRNet.

3.31.2. For interconnections among ISs operating at different classification levels (i.e., between unclassified and classified, unclassified and foreign national [or coalition] systems, etc.), developers and users refer to the CDS guidance, use only CDS-approved devices evaluated and validated through Certification Test and Evaluation or have a sufficient body of evidence to conduct a thorough risk analysis and adhere to CDS configuration guidelines.

**3.32. Cross-Domain Solutions.** The CDS process governs all interconnections of domains with different levels of protection. The purpose and procedures of CDS are extracted from DoD, DISA, National Security Agency (NSA), and the Unified Cross Domain Management Office policies and guidance. For guidance on the most current CDS process, reference CJCSI 6211.02, *Defense Information System Network (DISN): Policy, Responsibilities and Processes*. CDS is application specific. Visit the Air Force IA website for specific Air Force guidance.

**3.33. Mobile Code** . To protect ISs from the threat of malicious or improper use of mobile code, comply with the requirements in DoDI 8552.01, *Use of Mobile Code Technologies in DoD Information Systems*, and AFI 63-101 and AFI 33-210 for system acquisition and fielding. System developers and implementers follow guidelines in all applicable STIGs according to paragraph 3.12, Security Configuration and Implementation. Additional mobile code guidance is available at **https://iase.disa.mil/mcp/index.htmlH**.

**3.34. Ports, Protocols, and Services (PPS)** . The Air Force PPS Management Program provides policy on the use of PPS within the Air Force. Follow the requirements for the design, documentation, approval, registration, and implementation of PPS across Air Force enclave boundaries according to AFSSI 8551, *Ports, Protocols, and Services (PPS) Management*.

**3.35. Virtual Private Networks (VPN).** VPNs provide an encrypted means of transporting data across the Internet, NIPRNet, and within the AF-GIG.

3.35.1. All Air Force locations with an Air Force Service Delivery Point shall bulk encrypt all af.mil to af.mil traffic before it traverses the NIPRNet. This configuration is known as the Air Force VPN (AF-VPN). All traffic shall pass through the AF-VPN from Air Force base to Air Force base. Geographically Separated Units requiring a protected connection to the NIPRNet will submit requirement for connection behind a Main Operating Base to the Combat Information Transport System (CITS) Lead Command, HQ AFCA/ECN.

3.35.2. Follow i-TRM standards for VPN products and solutions. Obtain interim approval to use other VPN products/solutions (i.e., Community of Interest, encrypted tunneling, etc.) from SAF/XC prior to implementation. Solution must comply with current DoD requirements (i.e., Common Criteria, National Information Assurance Partnership Evaluation and Validation Program, etc.). Submit VPN solution to HQ AFCA/EAC to enter the review and approval process. Developers will use AF 4169 to request the exception.

3.35.3. VPN protection or solution approval does not relieve programs from completing required C&A according to AFI 33-210.

**3.36. Remote Access.**

3.36.1. User Functions. Comply with the guidelines in DISA's *Secure Remote Computing* STIG for end-user and limited (general) remote access.

3.36.2. Privileged (Administrative) Functions. Remote access for privileged functions is discouraged, permitted only for compelling operational needs and is strictly controlled. Comply with the guidelines in DISA's *Secure Remote Computing* STIG for administrative access and complete C&A requirements according to AFI 33-210 prior to implementation.

**3.37. Notice and Consent for Monitoring.** All DoD telecommunication systems are subject to monitoring by authorized personnel. Ensure all users are warned the systems they are entering are DoD telecommunications systems, and are provided with appropriate privacy and security notices to include statements informing them they are subject to monitoring, recording and auditing. Comply with AFI 33-219 (Section C) (will become AFSSI 8561) for specific telecommunications system requirements.

**3.38. IA Training and Certification.** Depending upon assigned duties, all military, civilian, and contractor personnel performing IA roles and responsibilities with Air Force ISs require specialized IA training and certification.

3.38.1. General Training Requirements.

3.38.1.1. For COMSEC training requirements see AFKAG-1N, (FOUO) *Air Force Communications Security (COMSEC) Operations*; AFI 33-201, Volume 2, (FOUO) *Communications Security (COMSEC) User Requirements* (will become AFSSI 4211, (FOUO) *Communications Security (COMSEC) User Requirements*; and AFI 33-201, Volume 9, (FOUO) *Operational Instruction for Secure Voice Devices* (will become AFSSI 4209, (FOUO) *Operational Instruction for the Secure Voice Devices).*

3.38.1.2. For EMSEC training requirements, see AFSSI 7700.

3.38.1.3. For DAA and other C&A training requirements, see AFI 33-210.

3.38.1.4. Several methods are available to supplement these training requirements: DISA provides CDs and DVDs, several vendors offer specialized IA courses, and other resources (including the Air Force Portal) provide computer-based training (CBT). Check the AF IA website for current information.

3.38.2. The *Air Force Implementation Plan For DoD 8570.01-M* provides guidelines for the official training and certification of personnel performing IA privileged user or management functions. This plan includes implementation guidance to:

3.38.2.1. Fully qualify privileged users and IAMs, through training and certification to DoD baseline requirements, to perform their IA duties.

3.38.2.2. Update IA privileged user or management requirements through appropriate manpower database and certification completion through appropriate personnel database. Civilian data is recorded in the Defense Civilian Personnel Data System. Military data is recorded with Special Experience Identifiers for Enlisted and with Experience Sets for Officers on the Unit Manning Document and in the Military Personnel Data System. Contractor certification requirements are identified in the respective statement of work.

3.38.2.3. Ensure collection of metrics and submission of reports to the Assistant Secretary of Defense for Networks and Information/DoD CIO to support planning and analysis of the IA workforce and annual FISMA reporting.

**3.39. IA Awareness and Education.** Authorized users will receive initial IA orientation and annual (every 12 months) awareness training to ensure they know, understand, and apply the IA requirements of Air Force information and ISs. The minimum orientation and awareness requirements for users are outlined in DoD 8570.01-M.

3.39.1. Air Force personnel using other than Air Force ISs 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 ISs will complete the Air Force training.

3.39.2. Users of Air Force ISs will complete refresher training prior to deploying if current training expires before the expected conclusion of the deployment.

**3.40. Security Rules of Behavior or Acceptable Use Policy.** The Air Force IA Awareness training describes the fundamentals of IA operations for Air Force information and ISs. The training outlines IA roles and responsibilities, expected behavior of all personnel, and consequences of inconsistent behavior or non-compliance. Completion of this training signifies user acknowledgement (understanding and acceptance) of the rules as a condition of access.

3.40.1. Depending upon the unique operating conditions or requirements of Air Force or other ISs, supplementary rules of behavior or acceptable use may be required. These rules must cover the same requirements (describe IA operations, delineate IA responsibilities and expected behavior, consequences of inconsistent behavior or non-compliance, etc.). Acknowledgement of the rules is also a condition of access to the IS.

3.40.2. If a user engages in conduct inconsistent with user IA awareness training, access to the information system may be suspended. Comply with the requirements in AFSSI 8522 for access suspension, reinstatement, or termination.

**3.41. Wireless Services.** Wireless services include but are not limited to wireless devices, systems, services, and technologies that are integrated or connected to DoD networks. The wireless services shall be considered part of the DoD networks (including systems for Joint use and Air Force systems that must interoperate directly with other Service or Coalition partner's networks).

3.41.1. They shall comply with:

3.41.1.1. The implementation guidance in DoD 8100.02.

3.41.1.2. The evaluation and validation requirements of DoDI 8500.2.

3.41.1.3. The C&A requirements of AFI 33-210.

3.41.1.4. Apply the guidelines in DISA's *Wireless* STIG for all wireless services and devices.

3.41.2. Wireless Local Area Networks (WLAN). WLANs will comply with the standard design developed by the CITS Program Office. Functional communities must procure WLAN compliant clients and ensure proper C&A of the system in accordance with AFI 33-210.

3.41.3. Wireless Wide Area Networks (WWAN). WWAN systems typically provide wireless broadband data services. Apply the guidelines in DISA's *Wireless* STIG for WWAN systems.

3.41.4. Radio Frequency Identification (RFID) Technologies. Comply with AFMAN 33-120, *Electomagnetic Spectrum Management*. Meet EMSEC requirements according to AFSSI 7700-series of publications.

3.41.5. Wireless Personal Area Network (WPAN). WPANs operate in the personal operating space of a user, which extends 10 meters in any direction. Examples of this technology include Bluetooth® devices. Apply the guidelines in DISA's *Wireless* STIG for WPANs.

3.41.6. Wireless Mice and Keyboards. Wireless keyboard and mice are widely available and use various wireless technologies such as WLAN, WPAN, Radio Frequency (RF), and Infra Red to transmit data to the computer. Wireless mice and keyboards must meet EMSEC requirements according to the AFSSI 7700-series of publications and comply with DISA's *Wireless* STIG.

**3.42. Portable Electronic Devices (PED).** PED is a generic title used to describe the myriad of small electronic items that are widely available. Almost all have wireless telecommunications capabilities that offer tremendous advantages for government users. It is becoming difficult to differentiate between these electronic devices as the trend is to combine capabilities and functions in various forms and format. Apply the general guidelines in DISA's *Wireless* and *Secure Remote Computing* STIGs for the use of PEDs. Comply with AFSSI 8502 for additional guidance on the use of PEDs in the computing environment.

**3.43. Voice Over Internet Protocol.** Comply with voice over Internet protocol requirements according to AFI 33-111, *Voice Systems Management*.

**3.44. Using Hardware or Software Not Owned by the Air Force.** Comply with the procedures of AFSSI 8502 before using public, contractor, other government service/agency, foreign, or private ISs to process sensitive or classified information.

**3.45. Secure Remote Computing and Telecommuting.**

3.45.1. The use of commercial (wired or wireless) ISP services for remote access is authorized provided the general guidelines in DISA's *Secure Remote Computing* STIG are followed for securing remote devices, including but not limited to workstations and PEDs.

3.45.2. Prior to implementing a telecommuting program, consult AFI 36-8002, *Telecommuting Guidelines For Air Force Reservists and Their Supervisors*. No further approval, beyond the requirements listed in AFI 36-8002, is required. Ensure vulnerabilities are assessed, with appropriate countermeasures employed, and documented in the C&A packages.

**3.46. Physical Security.**

3.46.1. Access to and Physical Protection of Computing Facilities. Employ physical security measures (i.e., access control, visitor control, physical control, testing, etc.) for network and computing facilities that process publicly releasable, sensitive, or classified information to only authorized personnel with appropriate clearances and a need-to-know according to AFI 33-115, Volume 1 and AFJI 31-102, *Physical Security*.

3.46.2. Workstation Security. Follow the procedures cited in AFSSI 8502 for workstation security in the computing environment.

**3.47. Information Security.** Comply with the requirements of AFI 31-401, *Information Security Program Management*, for workplace security procedures and storage of documents and IT equipment.

**3.48. Remanence Security.** All documents, equipment, and machine-readable media containing sensitive or classified data shall be cleared, sanitized, or destroyed before release to unauthorized personnel or outside DoD control (outside its security domain) according to AFSSI 5020, *Remanence Security* (will become AFSSI 8580, *Remanence Security*, and AFI 31-401.

**3.49. Environmental Controls.** Comply with environmental security requirements (i.e., lighting, fire, temperature/humidity, power, etc.) identified in IA controls that provide for both the availability and confidentiality of the information processed according to AFI 33-115, Volume 1.

**3.50. Protected Distribution System (PDS).** The transfer of national security information between controlled-access areas requires the use of NSA-endorsed products and services (see AFI 33-201, Volume 1 (FOUO) (will become AFSSI 4201 (FOUO) and AFSSI 7703, *Communications Security: Protected Distribution System [PDS]*).

**3.51. Exceptions, Deviations, and Waivers.** Exceptions, deviations, or waivers to this policy require documented justification from the DAA, using AF Form 4169. Exceptions, deviations, and waivers will then be forwarded to the OPR for the Air Force policy/implementation for further coordination or approval. Ensure the request makes a distinction between exceptions, deviations, and waivers.

3.51.1. An exception to policy is a temporary non-compliance with an expected fix date in the near term with mitigators in place.

3.51.2. A deviation to policy is a temporary or long-term, non-compliance with the use of a substitute measure to meet the requirement.

3.51.3. A waiver to policy is long term (sometimes permanent) non-compliance with appropriate mitigators (risk management) in place.

**3.52. A Plan of Action and Milestones (POA&M).** POA&M, also referred to as a corrective action plan, is distinct from exceptions, deviations, and waivers. POA&Ms assist security personnel in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in IT systems and programs. For more information on POA&Ms, reference C&A requirements in AFI 33-210.

***Section 3C—Information Collections, Records, and Forms or Information Management Tools (IMT)***

**3.53. Information Collections:** No information collections are created by this publication.

**3.54. Prescribed Forms:**

AF Form 4160, *Information Assurance Assessment and Assistance Program (IAAP) Criteria,*

AF Form 4167, *Two Person COMSEC Material Inventory*

AF Form 4168, *COMSEC Responsible Officer and User Training Checklist*

AF Form 4169, *Request for Waiver from Information Assurance Criteria*

AF Form 4170, *Emission Security Assessments/Emission Security Countermeasures Reviews*

AFCOMSEC Form 9, *Cryptographic Access Certificate*

**3.55. Adopted Forms:**

AF Form 847, *Recommendation for Change of Publication*

WILLIAM L. SHELTON, Lt Gen, USAF
Chief of Warfighting Integration and
Chief Information Officer

## Attachment 1

## GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

***References***

Public Law 100-235, *Computer Security Act of 1987*, January 8, 1988

5 USC § 552a

10 USC § 2224

44 USC § 3602

OMB Circular A-130, *Management of Federal Information Resources*

OMB Bulletin 90-08, *Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information*

Intelligence Community Directive (ICD) 503

CNSSI 4009, *National Information Assurance (IA) Glossary*

NSS 03-01, *Guidance for DoD Space Systems Acquisition Process*, 27 December 2004

National Security Telecommunications and Information Systems Security Advisory Memorandum TEMPEST/2-95, *Red/Black Installation Guidance*, 12 December 1995

DoDD 3200.12, *DoD Scientific and Technical Information (STI) Program (STIP)*, 11 February 1998

DoDD C-5200.5, *(C) Communications Security (COMSEC) (U)*, 21 April 1990

DoDD 8000.1, *Management of DOD Information Resources and Information Technology,* February 27, 2002; w/Change 1, March 20, 2002

DoDD 8100.01, *Global Information Grid (GIG) Overarching Policy*, 19 September 2002

DoDD 8100.2, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG)*, April 14, 2004

DoDD 8500.1, *Information Assurance (IA)*, October 24, 2002

DoDD 8581.1, *Information Assurance (IA) Policy for Space Systems Used by the Department of Defense*, 21 June 2005

DoDI 8500.2, *Information Assurance (IA) Implementation*, February 6, 2003

DoDI 8552.01, *Use of Mobile Code Technologies in DoD Information Systems*, 23 October 2006

DoDI 8580.1, *Information Assurance (IA) in the Defense Acquisition System*, 9 July 2004

DoD 5200.2-R, *Personnel Security Program*, 16 January 1987; through Change 3, 23 February 1996

DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, 19 December 2005

CJCSI 6211.02, *Defense Information System Network (DISN): Policy, Responsibilities and Processes,* 31 July 2003

CJCSI 6510.01D, *Information Assurance (IA) and Computer Network Defense (CND)*, 15 June 2004

CJCSM 6510.01, *Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)*, 25 March 2003; w/Change 1, 10 August 2004

AFPD 10-7, *Information Operations*, 6 September 2006

AFPD 13-3, *Air Force Network Operations (AFNetOps)*

AFPD 33-2, *Information Assurance (IA) Program,* 19 April 2007

AFI 10-710, *Information Operations Condition (INFOCON)*, 10 August 2006

AFI 10-901, *Lead Operating Command—Communications and Information Systems Management*, 22 March 2001

AFI 33-101, *Commanders Guidance and Responsibilities*

AFJI 31-102, *Physical Security*, 31 May 1991

AFI 31-401, *Information Security Program Management* 1 November 2005

AFI 31-501, *Personnel Security Program Management* 27 January 2005

AFI 33-100, *User Responsibilities and Guidance For Information Systems*

AFI 33-102, *Communications and Information Specialized Publications*, 17 July 2007

AFI 33-111, *Voice Systems Management*, 24 March 2005

AFI 33-114, *Software Management* 13 May 2004

AFI 33-115, Volume 1, *Network Operations (NETOPS)*, 24 May 2006

AFI 33-119, *Air Force Messaging*, 24 January 2005

AFI 33-129, *Web Management and Internet Use*, 3 February 2005

AFI 33-138, *Enterprise Network Operations Notification and Tracking*, 28 November 2005

AFI 33-401, *Implementing Air Force Architectures.* 14 March 2007

AFI 36-2201, Volume 1, *Training Development, Delivery, and Evaluation*, 1 October 2002

AFI 36-8002, *Telecommuting Guidelines for Air Force Reservists and Their Supervisors*, 1 July 1998

AFI 63-101, *Operations of Capabilities Based Acquisition System*, 29 Jul 05

AFKAG-1N, (FOUO) *Air Force Communications Security (COMSEC) Operations*, 27 January 2003

AFI 33-201, Volume 1, (FOUO) *Communications Security (COMSEC)*, 1 May 2005 (will become AFSSI 4201, (FOUO) *Communications Security(COMSEC)*

AFI 33-201, Volume 2, (FOUO) *Communications Security (COMSEC) User Requirements*, 26 April 2005 (will become AFSSI 4211, (FOUO) *Communications Security (COMSEC) User Requirements*

AFI 33-201, Volume 9, (FOUO) *Operational Instruction for the Secure Voice Devices*, 13 April 2005 (will become AFSSI 4209, *Operational Instruction for the Secure Voice Devices)*

AFI 33-210, *Certification and Accreditation (C&A) Program*

AFI 33-202, Volume 6, *Identity Management*, 23 May 2005 (will become AFSSI 8520, *Identification and Authentication)*

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)* (Chapter 6), 1 May 2006 (will become AFSSI 8561, *Information Assurance Notice and Consent)*

AFI 33-230, Information Assurance Assessment and Assistance Program (IAAP), 4 August 2004 [will become AFSSI 8560, *Information Assurance Assessment and Assistance Program (IAAP)]*

AFMAN 33-120, *Electomagnetic Spectrum Management*, 19 September 2006

AFMAN 33-214, Volume 1, *(S) Emission Security Assessments (U)*, 15 September 2003 (will become AFSSI 7701, *(S) Emission Security Assessments (U)*

AFMAN 33-223, *Identification and Authentication*, 29 July 2005 (will become AFSSI 8520, *Identification and Authentication)*

AFMAN 33-363, *Management of Records*, 1 March 2008

AFSSI 7700, *Emission Security*, 24 October 2007

AFSSI 7703, *Communications Security: Protected Distribution Systems (PDS)*, 26 August 2008

AFSSI 8502, *Computer Security*, 18 September 2008

AFSSI 8522, *Access to Information Systems*, 9 June 2008

AFSSI 8551, *Ports, Protocols, and Services (PPS) Management*, 5 November 2007

AFSSI 5020, *Remanence Security* (will become AFSSI 8580, *Remanence Security*)

*Air Force Records Information Management System Records Disposition Schedule (RDS)*

*Air Force Implementation Plan for DoD 8570.01-M* (will be come AFSSI 8570).

***Abbreviations and Acronyms***

**AFCA**—Air Force Communications Agency

**AF-DDA**—Designated Accrediting Authority for the Air Force-Provisioned Portion of the Global Information Grid

**AF-GIG**—Air Force-Provisioned Portion of the Global Information Grid

**AFI**—Air Force Instruction

**AFIOC**—Air Force Information Operations Center

**AFMAN**—Air Force Manual

**AFMC**—Air Force Materiel Command

**AFNOC**—Air Force Network Operations Center

**AFPD**—Air Force Policy Directive

**AFSPC**—Air Force Space Command

**AFSSI**—Air Force Systems Security Instruction

**AF**—VPN—Air Force Virtual Private Network

**AIS**—Automated Information System

**C&A**—Certification and Accreditation

**CBT**—Computer-Based Training

**CC**—Common Criteria

**CCB**—Configuration Control Board

**CDS**—Cross-Domain Solutions

**CI**—Counterintelligence

**CIO**—Chief Information Officer

**CITS**—Combat Information Transport System

**CJCSI**—Chairman of the Joint Chiefs of Staff Instruction

**CJCSM**—Chairman of the Joint Chiefs of Staff Manual

**CL**—Confidentiality Level

**CM**—Configuration Management

**CND**—Computer Network Defense

**CNSSI**—Committee on National Security Systems Instruction

**COMPUSEC**—Computer Security

**COMSEC**—Communications Security

**CoP**—Community of Practice

**COTS**—Commercial-Off-The-Shelf

**CTTA**—Certified TEMPEST Technical Authority

**DAA**—Designated Accrediting Authority

**DIACAP**—DOD Information Assurance Certification and Accreditation Process

**DISA**—Defense Information Systems Agency

**DISN**—Defense Information Systems Network

**DMZ**—De-militarized Zone

**DoD**—Department of Defense

**DoDD**—Department of Defense Directive

**DoDI**—Department of Defense Instruction

**DRU**—Direct Reporting Unit

**DSAWG**—DISN Security Accreditation Working Group

**EAL**—Evaluation Assurance Level

**EITDR**—Enterprise Information Technology Data Repository

**EMSEC**—Emission Security

**FISMA**—Federal Information Management Security Act

**FOA**—Field Operating Agency

**FOUO**—For Official Use Only

**GIG**—Global Information Grid

**IA**—Information Assurance

**IAAP**—Information Assurance Assessment and Assistance Program

**IAM**—Information Assurance Manager

**IAO**—Information Assurance Officer

**I&A**—Identification and Authentication

**INFOCON**—Information Condition

**IPO**—Information Protection Operations

**IS**—Information System

**ISP**—Internet Service Provider

**IT**—Information Technology

**JP**—Joint Publication

**KMI**—Key Management Infrastructure

**LAN**—Local Area Network

**MAC**—Mission Assurance Category

**MAJCOM**—Major Command

**NetD**—Network Defense

**NIPRNet**—Non-Secure Internet Protocol Router Network

**NSA**—National Security Agency

**NSS**—National Security System

**OMB**—Office of Management and Budget

**PDA**—Personal Digital Assistants

**PED**—Personal Electronic Device

**PEO**—Program Executive Officer

**PKI**—Public Key Infrastructure

**PM**—Program Manager

**POA&M**—Plan of Action and Milestones

**PPS**—Ports, Protocol, and Services

**RDS**—Records Disposition Schedule

**RF**—Radio Frequency

**RFID**—Radio Frequency Identification

**SAF**—Secretary of the Air Force

**SCI**—Sensitive Compartmented Information

**SIPRNet**—Secret Internet Protocol Router Network

**SOP**—Standard Operating Procedure

**STIG**—Security Technical Implementation Guide

**TAG**—Technical Advisory Group

**USC**—United States Code

**VPN**—Virtual Private Network

**WLAN**—Wireless Local Area Network

**WPAN**—Wireless Personal Area Network

**WWAN**—Wireless Wide Area Network

***Terms***

**Accreditation**—Formal declaration by a DAA that an IS is approved to operate in a particular security mode at an acceptable level of risk, based on the implementation of an approved set of technical managerial, and procedural safeguards.

**Automated Information System**—An AIS is a collection of hardware and software sharing a common set of security policies, procedures, and mechanisms. AISs may consist of a single stand-alone system, a central computer system with remote terminals (e.g., mainframe), a Local Area Network (LAN), or a Wide Area Network.

**Automated Information System Applications**—An AIS application is the product or deliverable of an acquisition program. An AIS application performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition. An AIS application may be a single software application (e.g., Integrated Consumable Items Support); multiple software applications that are related to a single mission (i.e., payroll or personnel); or a combination of software and hardware performing a specific support function across a range of missions (i.e., Global Command and Control System, Defense Messaging System). AIS applications are deployed to enclaves for operations, and have their operational security needs assumed by the enclave. Note that an AIS application is analogous to a "major application"; however, this term is not used in order to avoid confusion with the DoD acquisition category of Major Automated Information System. [DoDD 8500.1]

**Authentication**—Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

**Certification**—Comprehensive evaluation of the technical and nontechnical security features and countermeasures of an information system to establish the extent to which a particular design and implementation meet a set of specified security requirements.

**Client Support Administrator**—Person who insures functional communities of interest systems, servers, workstations, peripherals, communications devices, and software are on-line and supported.

**Common Criteria**—The International Common Criteria for Information Technology Security Evaluation (CC) defines general concepts and principles of IT security evaluation and presents a general model of evaluation. It presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems.

**Computer Network**—The constituent element of an enclave responsible for connecting computing environments by providing short-haul data transport capabilities (e.g., LAN) or long-haul data transport capabilities (i.e., operational, metropolitan, wide area, and backbone networks.

**Computing Environment**—A computer workstation or server (host) and its operating system, peripherals, and applications.

**Confidentiality**—The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

**Controls**—Prescribed actions taken to maintain the appropriate level of protection for information systems. Controls may validate security activities, detect security incidents and nonconformance, correct deficient security countermeasures, measure the assurance of information system activities, or report incidents. ( There are two divisions of control: management [policy, objectives, and criteria class] and internal [security requirements, mechanisms, and rules]. DODD 8000.1, February 27, 2002, w/Change 1, March 20, 2002, outlines internal controls for information systems.)

**Countermeasures**—Action, device, procedure, technique, or other measure that reduces the vulnerability of an information system.

**Cross-Domain Solutions (CDS)**—An IA solution that provides the ability to manually and/or automatically access and/or transfer data between two or more differing security domains.

**Defense-in-Depth**—The DoD approach for establishing an adequate IA posture in a shared-risk environment that allows for shared mitigation through: the integration of people, technology, and operations; the layering of IA solutions within and among IT assets; and, the selection of IA solutions based on their relative level of robustness. [DoDD 8500.1]

**Designated Accrediting Authority (DAA)**—Official with the authority to formally assume responsibility for operating an IS within a specified environment. [DoDD 8500.1, DoDI 8500.2, and AFPD 33-2]

**Enclave**—Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest MAC and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves are analogous to general support systems. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include LANs and the applications they host, backbone networks, and data processing centers. [DoDD 8500.1]

**Enclave Boundary**—The point at which an enclave's internal network service layer connects to an external network's service layer.

**Evaluation Assurance Level (EAL)**—One of seven increasingly rigorous packages of assurance requirements from CC, Part 3. Each numbered package represents a point on the CC's predefined assurance scale. An EAL can be considered a level of confidence in the security functions of an IT product or system.

**Foreign National**—Individual who is not a U.S. citizen, including U.S. military personnel, DoD civilian employees, and contractors. Sometimes referred to as local national, when the individual is employed in the country of which they are a citizen.

**Functional System**—Specific system used, owned, operated, and maintained by a functional community.

**Global Information Grid**—Globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes NSS as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DoD, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical, and business) in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems. Non-GIG IT is stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network. The GIG includes any system, equipment, software, or service that meets one or more of the following criteria: 1. Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services. 2. Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services. 3. Processes data or information for use by other equipment, software, and services. [DoDD 8100.01, ]

**Guest Information Systems**—Information systems which do not follow the normal AFCAP requirements for C&A. They may follow other DoD or Federal C&A processes such as NIST 800-37, DCID 6/3. They also include other DoD Agencies which have performed DIACAP and

are coming to the AF for connection to the Air Force provisioned portion of the GIG. These were formerly called Non-Air Force Information Systems. [AFI 33-210]

**Information Assurance Manager**—The individual responsible for the IA program of a DoD IS or organization. [DoDI 8500.2]

**Information Assurance Officer**—An individual responsible to the IAM for ensuring that the appropriate operational IA posture is maintained for a DoD IS or organization. [DoDI 8500.2]

**IA Product**—Product or technology whose primary purpose is to provide security services (i.e., confidentiality, authentication, integrity, access control or nonrepudiation of data); correct known vulnerabilities; and/or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks. Examples include such products as data/network encryptors, firewalls, and intrusion detection devices. [DoDD 8500.01]

**IA-Enabled Product**—Product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security-enabled messaging systems.

**IA Professionals**—Individuals performing IA duties and tasks. Positions these personnel fill are coded on the Unit Manning Document to indicate the required Information Assurance Workforce certification according to DoD 8570.01-M, , .

**Information**—1. Data derived from observing phenomena and the instructions required to convert that data into meaningful information. ( Includes operating system information [i.e., system parameter settings, password files, audit data, etc.]). 2. Facts, data, or instructions in any medium or form. [Joint Publication (JP) 1-02, ]. 3. The meaning that a human assigns to data by means of the known conventions used in their representation. [JP 1-02]

**Information Protection Operations (IPO)**—A critical subcomponent of the Network Management function that implements and enforces national, DoD, and Air Force security policies and directives. It provides proactive security functions established to assist Air Force organizations in deterring, detecting, isolating, containing, and recovering from IS and network security intrusions. The Network Control Center conducts IPO employing hardware and software tools to enhance the security of their networks.

**Information System**—A discrete set of information resources organized for collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes AIS applications, enclaves, outsourced IT-based processes, and platform IT interconnections. [DoDD 8500.1]

**Information System Security Engineering (ISSE)**—An engineering process that captures and refines information protection requirements and ensures their integration into IT acquisition processes through purposeful security design or configuration. [DoDI 8500.2]

**Integrity**—Property that allows the preservation of known unaltered states between baseline certifications and allows information, access, and processing services to function according to specified expectations. It is composed of data and system integrity.

**Information Technology**—Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control,

display, switching, interchange, transmission or reception of data or information by the DoD Component. For purposes of the preceding sentence, equipment is used by a DoD Component if the equipment is used by the DoD Component directly or is used by a contractor under a contract with the DoD Component that (1) requires the use of such equipment, or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. [DoDD 8100.01]

**IT Position Category**—Applicable to unclassified DoD ISs, a designator that indicates the level of IT access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. Position categories include: IT-I (Privileged), IT-II (Limited Privileged), and IT-III (Non-Privileged), as defined in DoD 5200.2-R). Investigative requirements for each category vary, depending on role and whether the incumbent is a U.S. military member, U.S. civilian government employee, U.S. civilian contractor, or a foreign national. The term IT Position is synonymous with the older term Automated Data Processing Position.

**Level of Protection**—Established safeguards with controls to counter threats and vulnerabilities based on the security requirements. Assures availability, integrity, and confidentiality of the IS.

**Mission Assurance Category**—Applicable to DoD ISs, the MAC reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. MACs are primarily used to determine the requirements for availability and integrity. DoD has three defined MACs (DoDD 8500.01):

**Mission Assurance Category I**—Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a category I system is unacceptable and could include the immediate and sustained loss of mission effectiveness. Category I systems require the most stringent protection measures. [DoDD 8500.01]

**Mission Assurance Category II**—Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. Category II systems require additional safeguards beyond best practices to ensure adequate assurance. [DoDD 8500.01]

**Mission Assurance Category III**—Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. Category III systems require protective measures, techniques or procedures generally commensurate with commercial best practices. [DoDD 8500.01]

**Mobile Code**—Mainstream software technology obtained from remote systems, transferred across networks, downloaded, and then executed on a local computer without explicit installation or execution by the recipient.

**Nonrepudiation**—Method by which the sender of data is provided proof of delivery and the recipient is assured of the sender's identity so that neither can deny having processed the data.

**Outsourced IT-based Process**—Outsourced IT-based process is a general term used to refer to outsourced business processes supported by private sector IS, outsourced IT, or outsourced information services. An outsourced IT-based process performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations. [DoDD 8500.1]

**Plan of Action and Milestones**—A POA&M is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

**Platform IT Interconnection**—Platform IT interconnection refers to network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition, and operations. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric. Examples of platform IT interconnections that impose security considerations include communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration. [DoDD 8500.1]

**Portable Electronic Device**—Any non-stationary electronic apparatus with the capability of recording, storing, and/or transmitting information. This definition includes, but is not limited to Personal Digital Assistants, cellular/PCS phones, two-way pagers, e-mail devices, audio/video recording devices, and hand-held/laptop computers. [DoDD 8100.2]

**Privileged User**—An authorized user who has access to system control, monitoring, or administration functions.

**Program Manager**—The person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the IS. (Synonymous with Single Manager or Project Manager.)

**Safeguards**—Protective measures and controls prescribed to meet the security requirements of an IS. ( Safeguards include security features and management constraints from the various security disciplines [i.e., administrative, procedural, physical, personnel, communications, emanations and computer security] used in concert to provide the requisite level of protection.).

**Security Feature**—A hardware-, firmware-, or software-controlled access protection to meet the security requirements of I&A; mandatory access control; discretionary access control; object reuse; or audit. Security features are a subset of IS security safeguards.

**Sensitive Information**—Information that the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Title 5 U.S.C. Section 552a (), but that has not been specifically authorized under criteria established by an Executive Order or an act of Congress to be kept secret in the interest of national defense or foreign policy. ( Systems that are not NSSs, but contain sensitive information are subject to be protected in accordance with the requirements of the Computer Security Act of 1987.)

**Specified Robustness**—The strength and level of confidence required of each IA solution is a function of the value of what is being protected (e.g., the mission assurance category or confidentiality level of the information being supported by the DoD IS) and the threat.

**Stand-Alone System**—An IS physically and electronically isolated from all other systems and intended to be used by one user at a time, with no data belonging to other users remaining on the system (e.g., a computer with removable storage media such as a floppy disk).

**System Integrity**—The attribute of a system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

**Threat**—Current and perceived capability, intention, or attack directed to cause denial of service, corruption, compromise, fraud, waste, or abuse to a system.

**User**—Person or process accessing an IS by direct connections (e.g., via terminals) or indirect connections.

**Vulnerability**—1. Weakness in an IS, or cryptographic system, or components (i.e., system security procedures, hardware design, internal controls) that could be exploited. 2. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. 3. The characteristics of a system which cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. [JP 1-02].

**Weapon System**—A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency. [JP 1-02]