

**17 JUNE 2004**



**Communications and Information**

**NETWORK AND COMPUTER SECURITY**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available digitally on the AFDPO WWW site at:  
<http://www.e-publishing.af.mil>

---

OPR: HQ AFCA/WFPS (MSgt David Hargitt)

Certified by: HQ USAF/XICI  
(Lt Col Yolanda Cruz)

Supersedes AFI 33-202, 30 August 2001;  
AFMAN 33-229, 26 September 2003

Pages: 73  
Distribution: F

---

This Air Force instruction (AFI) implements the computer security (COMPUSEC) portion of Air Force Policy Directive (AFPD) 33-2, *Information Protection* (will become *Information Assurance*), and establishes Air Force COMPUSEC requirements for information protection compliance with Public Law (P.L.) 100-235, *Computer Security Act of 1987*; 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 U.S. Code, Section 2224 (Defense Information Assurance Program), Department of Defense Directive (DoDD) 8500.1, *Information Assurance (IA)*, October 24, 2002; Department of Defense Instruction (DoDI) 8500.2, *Information Assurance (IA) Implementation*, February 6, 2003; DoDI 5200.40, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*, December 30, 1997; Department of Defense (DoD) 8510.1-M, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual*, July 31, 2000; and CJCSM 6510.01, *Defense-In-Depth: Information Assurance [IA] and Computer Network Defense [CND]*). The Uniform Code of Military Justice applies to personnel who violate the specific prohibitions and requirements of this instruction. This instruction gives the directive requirements for the COMPUSEC component of the Information Assurance (IA) discipline 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. 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. Additional instructions and manuals are listed on the Air Force Publishing web site at Uniform Resource Locator (URL): <http://www.e-publishing.af.mil> under Electronic Publications. Air Force Directory (AFDIR) 33-303, *Compendium of Communications and Information Terminology*, explains other terms. Direct questions or comments on the contents of this instruction, through appropriate command channels, to Headquarters Air Force Communications Agency (HQ AFCA/WFP), 203 W. Losey Street, Room 2200, Scott AFB IL 62225-5222. Refer recommended changes and conflicts between this and other publications to HQ AFCA/ITXD, 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, through appropriate channels, using AF Form 847, **Recommendation for Change of Publication**. Pro-

vide an information copy to HQ AFCA/WFP. Send any supplements to this publication to HQ AFCA/WFP for review, coordination, and approval prior to publication. Provide a copy of each final supplement to HQ AFCA/ITXD. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records*, and disposed of in accordance with Air Force Web-RIMS, *Records Disposition Schedule (RDS)* located at <https://webrims.amc.af.mil/rds/index.cfm>. Public Law 104-13, *The Paperwork Reduction Act of 1995* and AFI 33-360, Volume 2, *Content Management Program-Information Management Tool (CMP-IMT)*, affect this publication. 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 REVISIONS**

This update incorporates interim change (IC) 2004-1. The revision brings the foreign national administrator policy and the certifier criteria in-line with DoD policy. The other changes are administrative in nature and do not reflect policy change. A “|” indicates revised material since the last edition.

**Chapter 1—GENERAL INFORMATION 5**

- 1.1. Introduction. .... 5
- 1.2. Applicability. .... 5
- 1.3. Objectives. .... 5

**Chapter 2—ORGANIZATIONAL ROLES AND RESPONSIBILITIES 6**

- 2.1. Air Force Chief Information Officer (AF-CIO). .... 6
- 2.2. Assistant Secretary of the Air Force (Acquisition) (SAF/AQ). .... 6
- 2.3. Headquarters Air Force, Deputy Chief of Staff for Warfighting Integration (HQ USAF/XI). .... 6
- 2.4. Headquarters Air Force, Deputy Chief of Staff for Installations and Logistics, Director of Communications Operations (HQ USAF/ILC). .... 6
- 2.5. Headquarters Air Force Communications Agency (HQ AFCA). .... 6
- 2.6. Headquarters Air Intelligence Agency (HQ AIA). .... 7
- 2.7. Air Force Information Warfare Center (AFIWC). .... 7
- 2.8. Air Force Computer Emergency Response Team (AFCERT) .... 7
- 2.9. Headquarters Air Force Materiel Command (HQ AFMC). .... 7
- 2.10. Headquarters Air Force Space Command (HQ AFSPC). .... 8
- 2.11. Other Agencies Acquiring or Developing .... 8
- 2.12. Single Manager, Program Manager, or Project Manager .... 8
- 2.13. Designated Approving Authority (DAA). .... 9
- 2.14. Certifier. .... 9

2.15.	Major Commands (MAJCOM).	10
2.16.	Host	11
2.17.	Organizations.	13
2.18.	Foreign Disclosure Office.	14
<b>Chapter 3—BASIC INFORMATION</b>		<b>15</b>
3.1.	General.	15
3.2.	Common Criteria.	15
3.3.	Software Security.	15
3.4.	Product Assessments.	16
3.5.	Mobile Code.	16
3.6.	Configuration Management.	16
3.7.	Controlling Maintenance Activities.	16
3.8.	Malicious Logic Protection.	17
3.9.	Training.	18
3.10.	Notice and Consent for Information System Monitoring.	18
3.11.	Secret and Below Interoperability (SABI).	18
3.12.	Mission Assurance Categories	19
3.13.	Specified Robustness.	19
<b>Chapter 4—USE OF INFORMATION SYSTEMS</b>		<b>21</b>
4.1.	Desktops and Workstations.	21
4.2.	Multi-User Information Systems.	22
4.3.	Portable Electronic Devices (PED).	24
4.4.	Wireless Local Area Networks (WLAN).	27
4.5.	Remote Access via Modem.	29
4.6.	Using Hardware or Software Not Owned by the Air Force.	29
4.7.	Virtual Private Networks (VPN)	30
4.8.	Use of Multi-function Devices (MFD) on Unclassified Air Force Networks.	31
4.9.	Information Assurance Requirements.	31
<b>Chapter 5—ACCESS TO INFORMATION SYSTEMS AND NETWORKS</b>		<b>32</b>
5.1.	Access to Information Systems and Networks.	32
5.2.	Approving Foreign National Access and Use of Air Force Information Systems.	32

Table 5.1.	Approving Authority for Foreign National Access and Use of USAF Information Systems, Networks, Enclaves, and the NIPRNET. ....	33
5.3.	Connection By Stand-Alone System. ....	33
5.4.	Accessing the SIPRNET. ....	33
5.5.	Requirements for Volunteers on the Network. ....	33
<b>Chapter 6—</b>	<b>CERTIFICATION AND ACCREDITATION</b>	<b>35</b>
6.1.	Background. ....	35
6.2.	Individual Roles and Responsibilities ....	35
Table 6.1.	DAA Assignment. ....	36
6.3.	System Security Authorization Agreement (SSAA). ....	38
6.4.	Accreditation Decisions. ....	40
6.5.	Site Certification. ....	41
6.6.	Reporting: ....	41
6.7.	Information Collections, Records, and Forms or Information Management Tools (IMT). ....	41
<b>Attachment 1—</b>	<b>GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION</b>	<b>43</b>
<b>Attachment 2—</b>	<b>MOBILE CODE WAIVER PROCESS</b>	<b>55</b>
<b>Attachment 3—</b>	<b>EXAMPLE OF PDA USER AGREEMENT</b>	<b>56</b>
<b>Attachment 4—</b>	<b>DITSCAP - C&amp;A TASKS</b>	<b>58</b>
<b>Attachment 5—</b>	<b>INTERIM CHANGE 2004-1 TO AIR FORCE INSTRUCTION (AFI) 33-202, NETWORK AND COMPUTER SECURITY</b>	<b>60</b>

## Chapter 1

### GENERAL INFORMATION

**1.1. Introduction.** COMPUSEC is one of the IA disciplines promulgated in AFPD 33-2. Compliance ensures appropriate measures are taken to protect all Air Force information system resources and information effectively and efficiently. Appropriate levels of protection against threats and vulnerabilities for information systems prevent denial of service, corruption, compromise, fraud, waste, and abuse.

#### **1.2. Applicability.**

1.2.1. Applies to all information systems, including information system components of weapon systems, information systems that provide the management infrastructure and connections among other information systems, 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 Director of Central Intelligence Agency directive requirements governing Special Access Program information take precedence over this instruction.

1.2.3. This instruction is not applicable to Sensitive Compartmented Information (SCI) information systems. For SCI systems, refer to the Joint Department of Defense Intelligence Information Systems (DoDIIS)/Cryptologic SCI Information Systems Security Standards (JDCSISSS).

**1.3. Objectives.** The objectives of COMPUSEC are to protect and maintain the confidentiality, integrity, availability, authentication, and nonrepudiation of information system resources and information processed throughout the system's life cycle. These objectives will be met by provision of safeguard and their associated control collectively known as countermeasure.

1.3.1. Safeguards are actions or activities taken to protect information and are an integral part of security disciplines including COMPUSEC, Information Security, Emission Security (EMSEC), Communications Security (COMSEC), etc.

1.3.2. Associated controls are those administrative and management activities that implement and sustain the safeguards.

## Chapter 2

### ORGANIZATIONAL ROLES AND RESPONSIBILITIES

**2.1. Air Force Chief Information Officer (AF-CIO).** The AF-CIO is the responsible official for the Air Force owned and operated information systems in the Air Force enterprise.

2.1.1. Ensures that Information Assurance is an integral part of information systems and applications design, guaranteeing that appropriate systems security measures are in place and provided to protect mission data and system resources from all known threats.

2.1.2. Prior to fielding, ensures the necessary Command, Control, Communications, Computer and Intelligence (C4I) support requirements are documented in a C4I Support Plan (C4ISP).

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

2.2.1. Ensures IA related acquisition policy and guidance are considered in information systems acquisition, research and development, and contracts.

**2.3. Headquarters Air Force, Deputy Chief of Staff for Warfighting Integration (HQ USAF/XI).**

2.3.1. Responsible for the Air Force Network and Computer Security Program.

**2.4. Headquarters Air Force, Deputy Chief of Staff for Installations and Logistics, Director of Communications Operations (HQ USAF/ILC).** HQ USAF/ILC is the Air Staff focal point for day-to-day operations and maintenance of installation-level, intra-base, MAJCOM-oriented communications and information systems, inter-base telecommunications programs and systems supporting all non-tactical Air Force functions, as well as day-to-day O&M of long-haul networks. Further, it:

2.4.1. Develops policies and procedures for daily communication enterprise operations and maintenance.

2.4.2. Defines and promulgates training and certification standards for Air Force network professionals and establishes time lines that network professionals must maintain to meet Air Force standards.

2.4.3. Ensures the training and certification of Air Force network professionals and the training and licensing of Air Force network users according to paragraph 3.9.

2.4.4. Implements policies, develops supplemental guidance, and oversees installation level certificates for network operations.

2.4.5. Implements policies and oversees implementation of the Information Assurance Program including communications security, network and computer security, and emission security.

**2.5. Headquarters Air Force Communications Agency (HQ AFCA).** On behalf of HQ USAF/XI:

2.5.1. Reviews, evaluates, and interprets national and DoD COMPUSEC policy and doctrine, and makes recommendations on implementation to HQ USAF/XICI.

2.5.2. Develops, coordinates, and maintains HQ USAF/XI approved Air Force COMPUSEC instructions, manuals, and pamphlets.

2.5.3. Develops, coordinates, publishes, and maintains HQ USAF/XICI coordinated specialized COMPUSEC publications in accordance with AFI 33-206, *Air Force Specialized Information Assurance Publications*.

2.5.4. Provides guidance and support to MAJCOMs, FOAs, and DRUs in developing, implementing, and managing their COMPUSEC programs.

2.5.5. Manages the process of assessing government-produced and commercial-off-the-shelf software and hardware subsystem security features.

2.5.6. Develops applicable security techniques and procedures with Air Force-wide implications. Coordinates the information with HQ USAF/XICI and distributes this information to MAJCOMs.

2.5.7. Processes waiver or deviation requests to Air Force COMPUSEC policy and instructions.

2.5.8. Requests Air Force Information Warfare Center (AFIWC) assessment of security products.

2.5.9. Designated as the lead for managing the Air Force Secret and Below Interoperability (SABI) program. Advocates issues from customers with Air Staff and the SABI Secret Internet Protocol Router Network (SIPRNET) Connection Approval Office (SCAO) at Defense Information Systems Agency (DISA). Attends SABI meetings and participates in activities as required.

2.5.10. Identifies, defines and promulgates training requirements and certification standards for Air Force network professionals with HQ USAF/ILCXD.

## **2.6. Headquarters Air Intelligence Agency (HQ AIA).**

2.6.1. Provides guidance concerning security requirements and implementation of information systems in SCI facilities.

## **2.7. Air Force Information Warfare Center (AFIWC).**

2.7.1. Evaluates security products and provides assessment reports to HQ AFCA and applicable program management offices.

2.7.2. Develops Tactics, Techniques and Procedures (TTP) for use by the Air Force communications and information community.

## **2.8. Air Force Computer Emergency Response Team (AFCERT)**

2.8.1. Collects and analyzes technical vulnerability information. Develops countermeasures or requests assistance from appropriate agencies. Advises Air Force users on appropriate countermeasures.

2.8.2. Obtains and distributes IA threat and vulnerability information to appropriate users.

2.8.3. Assists Air Force organizations in evaluating information systems security, recommending IA countermeasures, developing IA requirements documents, and advocating funding furthering IA programs.

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

2.9.1. Assists HQ AFCA in developing COMPUSEC guidance and procedures for information systems in the acquisition and development life cycle.

2.9.2. Establishes IA training for Single Managers.

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

2.10.1. Assists HQ AFCA in developing COMPUSEC guidance and procedures for information systems in the acquisition and development life cycle.

2.10.2. Establishes IA training for Single Managers.

**2.11. Other Agencies Acquiring or Developing Information Systems or Software.** Assume single manager responsibilities (paragraph 2.12.) when developing systems or software outside a program management office structure.

## **2.12. Single Manager, Program Manager, or Project Manager .**

2.12.1. Ensures information systems acquired and developed comply with COMPUSEC policies and are assigned appropriate Mission Assurance Categories (see paragraph 3.12.).

2.12.2. Develops a Certification and Accreditation (C&A) plan and documents it in the System Security Authorization Agreement (SSAA).

2.12.3. Supports the C&A of information systems according to **Chapter 6** of this instruction.

2.12.4. Continuously identifies and analyzes threats and vulnerabilities to the information system and its data to maintain an appropriate level of protection.

2.12.5. Ensures design reviews address information system security requirements.

2.12.6. Establishes security controls to protect the information system during development.

2.12.7. Ensures information system life-cycle responsibilities are documented. This includes responsibility for reaccomplishing risk analysis, security testing, and certification due to modifications or changes to the system.

2.12.8. Ensures operating agencies receive copies of the SSAA documentation.

2.12.9. Ensures the SSAA documentation defines security procedures for system users, administrators, and maintainers.

2.12.10. Addresses all security-related issues to the System Security Working Group (SSWG) (see AFPAM 63-1701, *Program Protection Planning*).

2.12.11. Assists the Designated Approving Authority (DAA) in determining the sensitivity level of the information and the criticality of information system resources and information.

2.12.12. Plans and programs budgetary, manpower, and training support for the implementation and continuation of the COMPUSEC program to include improvements to security.

2.12.13. Ensures the DAA and users participate throughout the system development cycle in security analyses performed in conjunction with all design and specification reviews.

2.12.14. Ensures the appropriate coordination and review of all decisions concerning security trade-off and changes in requirements with the Certifier, system developers, users, and obtaining DAA approval (see AFPAM 63-1701).

2.12.15. Serves as the focal point for security system engineering during the system requirement definition, design, implementation, and testing phases of the program.

2.12.16. Ensures security measures are implemented to adequately satisfy the security specification and that any residual risks are identified.

2.12.17. Maintains C&A information in the Systems Compliance Database (SCD).

2.12.18. Reviews systems and applications to determine Public Key (PK)-enabling applicability. Maintains PK-enabled information in the SCD. **NOTE:** AFI 33-213, *DoD PKI Management and Use*, is currently being developed at the time of this version of AFI 33-202. AFI 33-213 will direct the use of the Department of Defense (DoD) Public Key Infrastructure (PKI). It will outline capabilities, assign responsibilities for the use and management of PKI functions within the Air Force, and establish Air Force PKI usage and registration requirements.

**2.13. Designated Approving Authority (DAA).** (**NOTE:** DAAs may be appointed for various information technology (IT) capabilities at differing levels [See [Table 6.1.](#)])

2.13.1. Ensures funding and manpower resources are allocated to achieve and maintain an appropriate level of protection and to remedy security deficiencies.

2.13.2. As necessary, appoints a DAA representative to deal with the day-to-day issues of accrediting information systems according to [Chapter 6](#).

2.13.3. Ensures a technically qualified Certifier is assigned to accomplish information system certification. Makes sure this individual is within the functional community and possesses the technical expertise on the information system being certified and on the security mechanisms in use. The certifier will not be in the wing or MAJCOM IA office.

2.13.4. Makes appropriate decisions to balance security requirements, mission, and resources against the defined or perceived threat. Determines the sensitivity level of the information and the criticality of information system resources and information.

2.13.5. Ensures resources are available to support the certification process and implementation of security countermeasures.

2.13.6. Is legally responsible for the secure operation of the information system to operate in a specific environment (see paragraph [6.2.1.3.](#)).

2.13.7. Ensures the security policy is developed and certification goals are clearly defined.

2.13.8. Is responsible for approving security requirement documents, Memorandums of Agreement, and deviations from security policy.

2.13.9. Accredits all information systems and applications under their authority prior to their operation.

2.13.10. Approves the use of freeware, shareware, or public domain software for information systems (see paragraph [3.3.2.](#)).

2.13.11. Ensures appropriate Mission Assurance Categories are assigned (see paragraph [3.12.](#)).

**2.14. Certifier.**

- 2.14.1. Is the formal certifying authority for the system and ensures the SSAA appropriately addresses the system security policy objectives for presentation to the DAA.
- 2.14.2. Leads certification teams formed to certify complex or large systems and networks.
- 2.14.3. Is a technical expert who makes technical judgments of an information system's compliance with the systems security policy and develops an accreditation recommendation for submission to the DAA based on system's certification.
- 2.14.4. Validates and assesses the risks associated with operating the system.
- 2.14.5. Provides C&A information to the program, single, functional, or project manager for input into the SCD.
- 2.14.6. Ensures appropriate Mission Assurance Categories are assigned (see paragraph 3.12.).

**2.15. Major Commands (MAJCOM).** Implements and manages a COMPUSEC program throughout the command. FOAs and DRUs electing to manage their own COMPUSEC program must provide documentation in a support agreement according to AFI 25-201, *Support Agreements Procedures*.

- 2.15.1. MAJCOM IA Office. Implements and oversees the MAJCOM COMPUSEC program.
  - 2.15.1.1. Prior to publication of any command supplement to Air Force COMPUSEC instructions and polices, provides copies to HQ AFCA/WFP and HQ AFCA/ITXD for review, coordination, and approval.
  - 2.15.1.2. Assists subordinate units in developing their COMPUSEC programs.
  - 2.15.1.3. Ensures communications and information system requirements documents include appropriate COMPUSEC requirements.
  - 2.15.1.4. Reviews audit, vulnerability, and security survey reports for applicability within the command. Implements measures to correct deficiencies.
  - 2.15.1.5. Ensures controls are in place to collect information system accreditation metrics data according to AFI 33-205, *Information Protection Metrics and Measurements Program*.
  - 2.15.1.6. Tracks and ensures compliance with C&A requirements for both classified and unclassified systems. Provides C&A guidance to the wing IA office.
  - 2.15.1.7. The MAJCOM focal point acts as the point of contact (POC) to DISA for the command regarding the Connection Approval Process.
  - 2.15.1.8. Provides a current list of SABI points of contact to HQ AFCA.
  - 2.15.1.9. Ensures MAJCOM IA Office and Wing IA Office personnel are knowledgeable with the Federal Acquisition Regulation (FAR); Defense Federal Acquisition Regulations (DFARS) and Air Force Federal Acquisition Regulations (AFFARS) information technology (IT) clauses and requirements.
- 2.15.2. MAJCOM Network Operations and Security Center (NOSC).
  - 2.15.2.1. Manages the MAJCOM infrastructure that provides the communications and information resources needed by customers to achieve their operational objectives.

2.15.2.2. Consults AFI 33-115, Volume 1, *Network Management* (will become *Network Operations*); Air Force Systems Security Instruction (AFSSI) 5021, *Time Compliance Network Order (TCNO) Management and Vulnerability and Incident Reporting*; and AFMAN 33-223, *Identification and Authentication*, for detailed descriptions of the IA roles performed at the NOSC.

**2.16. Host Wings.** Establish a base-wide COMPUSEC program administered by the wing IA office. Obtains assistance and guidance from the wing IA office for IA requirements and implementation (**NOTE:** ANG units co-located with active duty wings, but not in a host-tenant relationship, will have an independent DAA and establish an independent COMPUSEC program).

2.16.1. Host Base Communications Unit.

2.16.1.1. Communications and Information Systems Officer (CSO). Is normally the Communications Squadron Commander. Typically acts as the DAA Representative for Air Force information systems at the base level.

2.16.2. Wing IA Office.

2.16.2.1. Assists all base organizations and tenants in the development and management of their COMPUSEC programs. Provides training to Information System Security Officers (ISSO) (and Information System Security Managers (ISSM) to establish and maintain COMPUSEC programs.

2.16.2.2. Designates a focal point to track and ensure wing and tenant unit compliance with C&A requirements for both classified and unclassified information systems. Identifies noncompliant systems and get-well dates. Provides information to local Network Control Center (NCC) and MAJCOM IA office.

2.16.2.3. Semiannually verifies with the NCC that only accredited systems and applications (classified and unclassified) are connected to or use the base network.

2.16.2.4. Provides C&A guidance and assistance to wing and tenant units. Requests assistance from their MAJCOM.

2.16.2.5. Ensures information system requirements documents include appropriate COMPUSEC requirements.

2.16.2.6. Provides copies to their MAJCOM of any base supplements to Air Force COMPUSEC instructions and policies for review, coordination, and approval prior to publication.

2.16.2.7. Maintains appointment letters of all ISSMs and unit ISSOs.

2.16.2.8. Responds to suspected incidents of contaminated systems. Ensures remanence security is implemented according to AFSSI 5020, *Remanence Security*.

2.16.2.9. Collects and reports metric data according to AFI 33-205.

2.16.2.10. Conducts IA self-assessment and provides assistance to units according to AFI 33-230, *Information Protection Assessment and Assistance Program* (will become *Information Assurance Assessment and Assistance Program*).

2.16.2.11. Maintains familiarity with new technologies and policies by attending COMPUSEC-related conferences, working groups, etc.

2.16.2.12. Ensures a role-based access scheme that accounts for all privileged access and implements the principles of least privilege and separation of functions is utilized. Users shall access

only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.

2.16.2.13. Maintains visibility over all privileged user assignments to ensure separation of functions and compliance with personnel security criteria established in DoD 5200.2-R, *Personnel Security Program*. Assignment to privileged user roles with IA management access shall be accomplished in accordance with DoDI 8500.2 (see table E3.T1).

2.16.2.14. Reviews and coordinates IT security related specification and requirements identified in contracting documents.

2.16.3. Network Control Center (NCC), Network Operations and Security Center (NOSC), and Network Operation activities.

2.16.3.1. Manages the local (or enterprise) infrastructure that provides customers the communications and information resources needed to achieve their operational objectives.

2.16.3.2. Complies with the IA roles and responsibilities outlined in AFI 33-115, Volume 1.

2.16.4. Information System Security Manager (ISSM).

2.16.4.1. Is the primary technical representative for the DAA (or DAA Representative) for issues affecting the enclave. ISSM is synonymous with information assurance manager (IAM); normally this individual will reside within the wing IA office or the NCC (see [Attachment 1](#), Terms). Individuals in this position must be US citizens (see DoDI 8500.2 for additional information).

2.16.4.2. Is the single liaison between the enclave and the wing IA office for network core services COMPUSEC matters. Only one ISSM will exist for each enclave (i.e., base network or local enclave).

2.16.4.3. Coordinates with wing IA office to ensure all users and ISSOs (under their purview) receive COMPUSEC training according to paragraph [3.9](#).

2.16.4.4. Provides a copy of appointment letter (signed by DAA or DAA representative) to the wing IA office.

2.16.4.5. Ensures ISSOs are assigned to functional systems or on a system-by-system basis.

2.16.4.6. Provides C&A information to the wing IA office for appropriate tracking.

2.16.4.7. Develops and implements a role-based access scheme that accounts for all privileged access and implements the principles of least privilege and separation of functions. Users shall access only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.

2.16.4.8. Ensures audit trail records from all core network services and infrastructure devices are regularly reviewed for indications of inappropriate or unusual activity. Suspected violations of IA policies are analyzed and reported in accordance with DoD, Air Force and MAJCOM reporting procedures.

2.16.4.9. Will be a member of any appropriate Configuration Control Boards (CCB) or steering groups.

**2.17. Organizations.** Commanders must appoint in writing an ISSO to supervise the unit COMPUSEC program. Additional (subordinate) ISSO positions may be assigned for additional support at the discretion of local units; however, only one ISSO is required.

2.17.1. Information Systems Security Officer (ISSO) (formerly the Unit COMPUSEC Manager, ISSO is also synonymous with information assurance officer (IAO)). Individuals in this position must be US citizens (see DoDI 8500.2 for additional information).

2.17.1.1. Is the single liaison between the unit and the ISSM or wing IA office for COMPUSEC matters (these duties could be accomplished by the workgroup manager). Implements COMPUSEC program to ensure compliance with the provisions of this instruction, including any MAJ-COM or wing supplements. (**NOTE:** All actions listed below may not be applicable to each ISSO; however, the ISSO must ensure applicable actions are being accomplished)

2.17.1.2. Establishes controls to ensure users operate, maintain, and dispose of information systems according to the current system security policy and existing policy and procedures.

2.17.1.3. Ensures procedures are in place for users to notify the ISSO or alternate if problems arise during critical or classified processing.

2.17.1.4. Ensures the system security policy for each information system is available to all users.

2.17.1.5. Establishes controls to ensure audit trails are periodically reviewed for all systems under the ISSO's control.

2.17.1.6. Performs an initial evaluation of each vulnerability or incident, and begins corrective or protective measures and reports according to AFSSI 5021.

2.17.1.7. Evaluates known vulnerabilities to ascertain if additional safeguards are needed to protect information systems.

2.17.1.8. Ensures all network and system administrators are taking aggressive action to implement TCNOs within the mandatory timeframe and comply with the vulnerability and incident reporting procedures outlined in AFSSI 5021.

2.17.1.9. Ensures users receive COMPUSEC training on system-specific security procedures.

2.17.1.10. Periodically validates user-access privilege levels.

2.17.1.11. Maintains the accreditation according to [Chapter 6](#).

2.17.1.12. Ensures organizations do not use freeware, shareware, or public domain software unless approved for use by the DAA. The ISSO ensures the software is free of viruses, hidden defects, and obvious copyright infringements. The ISSO coordinates vulnerability testing on all proposed software and hardware changes.

2.17.1.13. Monitors information system activities to ensure system integrity; establishes reaction and maintenance controls for the facility; and performs system access or revocation tasks.

2.17.1.14. Continually identifies threats, deficiencies, and associated countermeasures.

2.17.1.15. Reports system security incidents, classified message incidents, vulnerabilities, and virus attacks according to AFSSI 5021.

2.17.1.16. Establishes restrictions on shared use of programs or files.

- 2.17.1.17. Ensures site certification is obtained before operational use.
- 2.17.1.18. Ensures each information system operates within the constraints of the system security policy and network security policy (**NOTE**: Any deviations must be approved by the cognizant DAA).
- 2.17.1.19. Ensures measures exist to control access to information systems based on users validated clearances, access approval for categories, and need to know.
- 2.17.1.20. Maintains information systems processing sensitive, classified, and critical information according to configuration management controls, and provides security guidance to the appropriate CCB or steering group.
- 2.17.1.21. Identifies information ownership for each multi-user information system to include accountability, access rights, and special handling requirements.
- 2.17.1.22. Ensures information systems are cleared or sanitized according to AFSSI 5020.
- 2.17.2. Users: In addition to following policy outlined in DoDI 8500.2, all users must:
  - 2.17.2.1. Be licensed in accordance with AFI 33-115, Volume 2, *Licensing Network Users and Certifying Network Professionals*, and ensure they receive Information Assurance Awareness Training according to AFI 33-204, *Information Assurance Awareness Program*. **NOTE**: ANG personnel may be certified to use ANG networked resources by completing equivalent training.
  - 2.17.2.2. Protect system information and resources according to established security policies and procedures.
  - 2.17.2.3. Report system security incidents, classified message incidents, vulnerabilities, and virus attacks to the ISSO according to AFSSI 5021.
  - 2.17.2.4. Maintain current antivirus software and obtain ISSO approval before disabling or changing the approved antivirus software.
  - 2.17.2.5. Not install any software or hardware without coordination with the ISSO or workgroup manager.

**2.18. Foreign Disclosure Office.** Authorizes foreign national access to classified and controlled unclassified information.

## Chapter 3

### BASIC INFORMATION

**3.1. General.** Safeguard information systems and information against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or release to unauthorized persons. Protect hardware, firmware, software, and information against unauthorized disclosure, destruction, or modification.

**3.2. Common Criteria.** Common Criteria is a formal specification of security functionality and assurance requirements that forms the cornerstone for reliable and repeatable testing and evaluation of security-enhanced Information Technology products. The Common Criteria standard is a primary vehicle for specifying security requirements in user Protection Profiles and developer Security Targets.

3.2.1. Information on US Government recommended products which have been determined to be compliant with Protection Profiles or Security Targets certified by National Security Agency (NSA) as appropriate for use in "national security" systems (as defined in AFI 33-201, (FOUO) *Communications Security [COMSEC]*) consistent with the environments specified in the Protection Profiles or Security Targets is available at National Information Assurance Partnership (NIAP) home page (<http://niap.nist.gov/>).

3.2.2. System owners use Common Criteria for guidance when determining required levels of assurance and for guidance and reference when formulating statements of requirements for security functions. System security assurance requirements are used to establish a set of assurance components in standard Evaluation Assurance Levels (EAL). Evaluation criteria for Protection Profiles and Security Targets are used to assign appropriate EAL ratings, from EAL1 to EAL7.

3.2.3. Functional system and computer application owners must ensure the Common Criteria with approved Protection Profiles and Security Targets are used to conduct Security Test and Evaluations. They must also ensure an SSAA and a C4ISP are developed. The SSAA and the C4ISP are the primary documents supporting the Certificate of Networkiness (CoN) and Certificate to Operate (CtO) assessment processes.

3.2.4. Network enclave and standalone system owners must ensure the Common Criteria is used when purchasing IT security products for their systems. Products used must be documented in SSAAs for the C&A and approved by the DAA.

3.2.5. Further information on the Common Criteria activities can be obtained at NIAP home page (<http://niap.nist.gov/>).

### 3.3. Software Security.

3.3.1. Ensure all software is included in the SSAA for the system. Reference paragraph 6.3. for additional information.

3.3.2. Freeware, public domain software, and shareware originating from questionable or unknown sources, [e.g., World Wide Web sites] are highly susceptible to malicious logic and may violate the system security policy. If no alternative IT solutions are available, base use of such software on operational need, perform vulnerability testing on the software, and receive approval to use from the DAA. Do not use trial or demo software.

3.3.3. Avoid software development, testing, and debugging on operational information systems. If no alternate exists, the following conditions must be met:

3.3.3.1. Protect applications and data from unauthorized disclosure.

3.3.3.2. Maintain the availability, confidentiality, integrity, and accountability of system resources and information.

3.3.4. Do not use foreign country software that does not meet restrictions laid out by the Buy American Act and Trade Agreements Act; ensure you consult with your contracting office and communications squadron prior to any purchase.

**3.4. Product Assessments.** Send requests to recommend security products to HQ AFCA/WFP. AFIWC will conduct product assessment at the request of HQ AFCA/WFP.

**3.5. Mobile Code.** Mobile Code is a 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.

3.5.1. To protect DoD systems from the threat of malicious or improper use of mobile code, the Assistant Secretary of Defense for Networks and Information Integration (ASD/NII, previously the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD/C3I)) released policy guidance that limits the use of mobile code on DoD information systems. This policy guidance is applicable to all Air Force information systems. A copy of this guidance is available at <http://www.c3i.osd.mil/org/cio/doc/mobile-code11-7-00.pdf>. The AF-CIO is responsible for the Air Force owned and operated functional systems and approval of waiver requests cannot be delegated below this level. See **Attachment 2** for the procedures to request a mobile code waiver.

3.5.2. Disable ActiveX and Java applets when connecting to untrusted sites (non-.gov or -.mil sites). When mission accomplishment necessitates the need to enable these features, obtain DAA approval and update the SSAA.

**3.6. Configuration Management.**

3.6.1. Use configuration management to ensure the integrity of critical functions in security-related hardware, firmware, and software of all information systems. Distribute hardware, firmware, and software under configuration management control to provide an appropriate level of protection and assure product integrity. Use the computer resources life-cycle management plan and the CCB to ensure system integrity throughout the life cycle of an information system.

3.6.2. Ensure interoperability and compatibility with existing Air Force standard network security policies and procedures according to the Air Force Infostructure Technical Reference Model (i-TRM).

**3.7. Controlling Maintenance Activities.**

3.7.1. Restrict information system maintenance to authorized personnel with a security clearance for the highest classification and most restricted category of information processed. Uncleared individuals may perform maintenance on information systems used to process classified information only if the information is sanitized or an appropriately cleared individual (capable of identifying unauthorized activity) monitors their actions to prevent unauthorized disclosure.

3.7.2. Allow remote software diagnostics or maintenance only if the information system audits such activities or an appropriately cleared individual (capable of identifying unauthorized activity) observes such activities. When maintenance activities are suspended or completed, disconnect or disable access to the information system. Additionally, verify the identity of the maintenance personnel to prevent the unauthorized disclosure of sensitive and classified information.

3.7.3. Prevent vendor maintenance personnel from removing classified or sensitive media, products, etc., from government facilities when those personnel do not have the proper authorization (e.g., verified identity, security clearance, access approval for categories, need to know) to access that media. Before releasing an information system component containing nonvolatile storage media (e.g., tapes, disks, battery-powered random access memory, etc.) to uncleared maintenance activities, sanitize the component of classified and sensitive information according to AFSSI 5020.

**3.8. Malicious Logic Protection.** Protect information systems (including network servers) from malicious logic (e.g., 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. At a minimum:

3.8.1. Implement DoD approved antivirus software on all information systems and networks.

3.8.1.1. Use only antivirus tools and signature files/datfiles obtained from the AFCERT file transfer protocol (FTP) or DoD Computer Emergency Response Team (CERT) web sites. NCCs will direct configuring (where technically feasible) the signature file update routine to NCC-controlled site inside the base security perimeter.

3.8.1.1.1. The use of additional antivirus software (in conjunction with DoD approved antivirus software) may be approved by the DAA. A waiver is required if DoD antivirus software is available and not used. Forward waiver requests through your chain of command to HQ AFCA/WFP for approval or disapproval.

3.8.1.2. Activate antivirus software during information system use (auto-defend or auto-protect must be enabled to perform a scan when a file is run, opened, copied, moved, created, or downloaded).

3.8.1.3. Information Protection Operations (IPO) personnel in the NCC will check for antivirus signature files/datfiles updates daily from the AFCERT/DoD CERT sites. Users will pull down new signature files from the NCC-controlled site or NCC's site will replicate (if feasible) new signature files to the users as soon as received. Accomplish a virus scan immediately following an update of a signature file.

3.8.1.4. Establish procedures to rapidly obtain, distribute, and install changes to antivirus software on all information systems (including network servers).

3.8.1.5. Unless waived by the DAA, filter E-mail at the base perimeter for visual basic (.vbs), executable (.exe), and other attachments conducive to the propagation of malicious logic.

3.8.2. Where feasible, scan all incoming traffic and files for viruses at the network server level.

3.8.3. Scan removable and fixed media:

3.8.3.1. Through use of auto-defend or auto-protect settings. If antivirus software cannot be set then an antivirus scan must be invoked daily on all files on all servers (and workstations).

3.8.3.2. According to the local virus scanning frequency for fixed media information systems (e.g., laptops, desktop computers) established by the DAA or DAA Representative. The time period between scans will not exceed 7 calendar days. If a local scanning frequency is not established in the host wing's network security policy, scan all fixed media daily.

3.8.3.3. Scan removable media for viruses before each use. This scan can be automated if anti-virus software is configured properly.

3.8.4. Report all virus attacks according to AFSSI 5021.

3.8.5. Preserve malicious logic reports as evidence for ongoing investigations.

3.8.6. Include virus prevention, detection, eradication, and reporting procedures in user training.

### **3.9. Training.**

3.9.1. License network users (see paragraph [2.17.2.](#)).

3.9.2. The wing IA office provides training on network and computer security, identification and authentication, remanence security, vulnerabilities and incidents reporting, etc.

3.9.3. The DAA (or DAA Representative) will ensure training of key players in Information Assurance (e.g., DAA, ISSM/O, Certifier etc.)

3.9.3.1. Several methods are available to assist in meeting training requirements: DISA provides CD-ROMs, several vendors offer courses and computer-based training (check AFCA homepage for current information).

**3.10. Notice and Consent for Information System Monitoring.** Information systems are subject to monitoring by authorized personnel. Display warning banners according to AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*.

**3.11. Secret and Below Interoperability (SABI).** . The purpose and procedures of SABI are extracted from DoD, DISA and NSA policies. The SABI process governs all interconnections of domains with different levels of protection. This includes not only unclassified to Secret interconnections, but unclassified to foreign national systems (coalition disseminations) as well.

3.11.1. HQ AFCA manages and provides day-to-day operational support for the SABI Program. HQ AFCA advocates Air Force SABI requests, votes on SABI initiatives and supports enhancements to improve the SABI Program. Air Staff provides representation for the Defense Information Systems Network (DISN) Security Accreditation Working Group (DSAWG), which oversees the SABI and Community Risk aspects to ensure the development and availability of needed capabilities and guidance for DoD C4I systems. HQ AFCA assists in identifying, reviewing, and validating DoD C4I security requirements to help manage risks. Where appropriate, recommend DoD community risk policies, procedures, and initiatives as required. Promote the development and coordination of certification and accreditation criteria, guidelines, and policies for employment by the user community to balance the mission/operational requirement with costs. Identify and articulate issues relating to interoperability and standardization of trusted C4I systems. Promote the development of, and compliance with, common criteria, security standards and open system concepts to ensure interoperability, commonality, and affordability of secure C4I systems in support of the local DAA and DoD at large. And finally, HQ AFCA monitors and coordinates the community risk management initiatives of the Combatant

Commanders/ Services/Agencies and recommends priorities to the United States Military Communications-Electronic Board Information Assurance Program for community risk activities.

3.11.2. SABI requests are made via the Global Information Grid (GIG) Interconnection Approval Process (GIAP)/SABI web site. The GIAP/SABI Web site requires individual SIPRNET access. HQ AFCA/WFP provides an orientation program at the Air Force Information Protection web site under the title of "HQ AFCA SABI Briefing."

3.11.3. HQ AFCA/WFP will advocate issues from Air Force customers with Air Staff and the DISA SCAO. Air Force MAJCOM/FOA/DRU customers are requested to contact HQ AFCA/WFP with problems or when questioning status of their SABI request/tickets. Allow 60 days from the time of the request before inquiring on status.

**3.12. Mission Assurance Categories .** All DoD information systems shall be assigned a mission assurance category that is directly associated with the importance of the information they contain relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission (see DoDD 8500.1 and DoDI 8500.2). Requirements for availability and integrity are associated with the mission assurance category, while requirements for confidentiality are associated with the information classification or sensitivity and need-to-know. Both sets of requirements are primarily expressed in the form of IA controls and shall be satisfied by employing the tenets of defense-in-depth for layering IA solutions within a given IT asset and among assets; and ensuring appropriate robustness of the solution, as determined by the relative strength of the mechanism and the confidence that it is implemented and will perform as intended. The IA solutions that provide availability, integrity, and confidentiality also provide authentication and nonrepudiation.

**3.13. Specified Robustness.** In order to ensure that each component of an IA solution is correctly implementing its intended security services and is protecting its information from the identified threat, each component within the network system needs to provide an appropriate level of robustness.

3.13.1. Robustness describes the strength of mechanism (e.g., the strength of a cryptographic algorithm) and assurance properties (i.e., confidence measures taken to ensure proper mechanism implementation) for an IA solution. The more robust a particular component is, the greater the level of confidence in the protection provided to the security services it supports. It is also possible to use non-technical measures to achieve the equivalent of a level of robustness. For example, physical isolation and protection of a network can be used to provide confidentiality. In these cases, the technical solution requirement may be reduced or eliminated. There are three levels of robustness (additional information is available in DoDI 8500.2):

3.13.1.1. High robustness security services and mechanisms provide, through rigorous analysis, the most confidence in those security mechanisms. Generally, high robustness technical solutions require NSA-certified high robustness solutions for cryptography, access control and key management and high assurance security design as specified in NSA-endorsed high robustness protection profiles, where available.

3.13.1.2. Medium robustness security services and mechanisms provide for additional safeguards above Basic. Medium robustness technical solutions require, at a minimum, strong (e.g., crypto-based) authenticated access control, NSA-approved key management, National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS)-validated

cryptography, and the assurance properties as specified in NSA-endorsed medium robustness protection profiles or the Protection Profile Consistency Guidance for Medium Robustness.

3.13.1.3. Basic robustness security services and mechanisms are usually represented by good commercial practice. Basic robustness technical solutions require, at a minimum, authenticated access control, NIST-approved key management algorithms, NIST FIPS-validated cryptography, and the assurance properties specified in NSA-endorsed basic robustness protection profiles or the Protection Profile Consistency Guidance for Basic Robustness.

## Chapter 4

### USE OF INFORMATION SYSTEMS

**4.1. Desktops and Workstations.** This section applies to all information systems used by only one individual at a time. The desktop or workstation may be operated as a stand-alone system or connected in a network environment. (**NOTE:** Information systems that allow file sharing over a network must comply with the requirements of multi-user information systems [paragraph 4.2].)

#### 4.1.1. Unclassified and Sensitive Processing:

4.1.1.1. Verify each user's need for access to information system resources and information. Follow identification and authentication procedures according to AFMAN 33-223 and AFI 31-501, *Personnel Security Program Management*.

4.1.1.2. Confirm that information systems attached to the network comply with the network security policy.

4.1.1.3. Protect against casual viewing of information by using password-protected screen savers and by requiring users to remove their Common Access Card (CAC) from the reader when workstations are unattended. Users must ensure workstation locks when CAC is removed.

4.1.1.4. Protect the information system and data against tampering. Provide protection from outsider threats by controlling physical access to the information system itself. Provide protection from insider and outsider threats by using CAC removal lock feature, installing keyboard locks, password-protected screen savers, add-on security software, etc., or by establishing controls for removal and secure storage of information from unattended information systems. Users of DoD PKI software certificates must use the CTRL-ALT-DEL and lock their workstations when leaving them, or log out of their applications and network domain.

4.1.1.5. Use protection measures in paragraph 4.1.1.4. and use appropriate network operating system security features to force each workstation to log onto the network before granting access to network services and resources.

4.1.1.6. Clear or sanitize media used to store sensitive or classified information before release to unauthorized personnel or outside DoD control. Follow procedures in AFSSI 5020.

4.1.1.7. Do not connect or subscribe to commercial Internet service providers (ISP) for official E-mail or network services. Commercial ISP service can only be obtained via waiver from HQ USAF/ILC and the DoD GIG board. Waiver requests shall explain how the other than Non-Secure Internet Protocol Router Network (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.

4.1.1.8. Adhere to the DISA Connection Approval Process if the system is connected to the NIPRNET. Connection Approval Process information can be found at <https://iase.disa.mil/CAP/index.html>.

4.1.1.9. Users are responsible for backing up their data. Frequency of back-ups may be determined by local policy, or if allowed by local policy, by the user based on criticality of the information.

4.1.2. Classified Processing. In addition to the security requirements in paragraph 4.1.1., the following security requirements apply:

4.1.2.1. Physically protect each network connection to a level appropriate for protecting the most restricted information accessible at the network access point.

4.1.2.2. Information systems using nonvolatile, nonremovable storage media must meet one of the following conditions:

4.1.2.2.1. Install the computer in an area approved for open storage of information at or above the highest classification level of the information processed.

4.1.2.2.2. Use a National Computer Security Center (NCSC)-evaluated, AFCA-assessed, or locally tested and DAA-approved (if no approved method or technique is available) product or technique to prevent storing classified information on nonvolatile, nonremovable storage media. Ensure product protects against inadvertently writing information to storage media.

4.1.2.3. Unless multi-level security is implemented, ensure all personnel authorized to use the information system are cleared to the highest level and most restricted category of information contained in the information system.

4.1.2.4. Use a separate copy of the operating system and other necessary software for each level of classification on information systems employing periods processing (see [Attachment 1](#), Terms).

4.1.2.5. Clear equipment and media when changing modes of operation or changing operations to the same or higher classification level. Sanitize storage devices that contain classified information before using at a lower classification level according to AFSSI 5020. Once unclassified media is introduced into a classified computer, the media becomes classified at the same classification level as the system. Media may remain unclassified only if the write protect mechanism (or process) has been clearly enabled and tested to prevent classified information from writing to the unclassified media.

4.1.2.6. Safeguard, mark, and label output products and removable media according AFI 31-401, *Information Security Program Management*.

4.1.2.7. Provide internal markings on files to indicate the information sensitivity level and any special handling instructions, where practical.

4.1.2.8. Meet EMSEC requirements according to AFI 33-203, *Emission Security*.

4.1.2.9. Adhere to the DISA Connection Approval Process if the system is connected to the SIPR-NET. Connection Approval Process information can be found at <https://iase.disa.mil/CAP/index.html>.

**4.2. Multi-User Information Systems.** This section applies to all multi-user file servers (e.g., FTP, network file servers, World Wide Web servers, etc.), and information systems that permit file sharing, perform network security functions, or provide security services (e.g., Automated Security Incident Monitoring [ASIM], firewalls, etc.). AFI 33-115, Volume 1, directs that all communications and information services entering and exiting the base or site fall under the operational control of the NCC or NOSC. Follow Air Force Technical Orders, AFI and/or AFMAN procedures, AFCA guidance and other relevant

publications on implementing network boundary protection to include the ASIM system, installing and configuring firewalls, and disabling system services.

4.2.1. **Unclassified and Sensitive Processing.** In addition to the security requirements listed in paragraph 4.1.1., the following security requirements apply. If conflicts develop, the following requirements take precedence:

4.2.1.1. Adhere to AFMAN 33-223 to ensure individual accountability and use of proper identification and authentication (I&A) procedures, and verify access.

4.2.1.2. Control access to files, software, and devices so that only authorized users can use them.

4.2.1.3. Control access to prevent unauthorized persons from using network facilities.

4.2.1.4. Use network components (e.g., trusted routers, bastion hosts, gateways, firewalls, etc.) or information systems that enforce media access control (MAC) and I&A to provide access controls.

4.2.1.5. Provide each user with only those system privileges needed for assigned tasks (least privilege concept).

4.2.1.6. Limit access to privileged programs (i.e., operating system, system parameter and configuration files, and databases), utilities (i.e., assemblers, debuggers, maintenance utilities), and security-relevant programs/data files (i.e., security monitor, password files, and audit files) to authorized personnel (i.e., system administrator and ISSO).

4.2.1.6.1. Air Force servers storing passwords, when software is available, shall run password enforcement software to conform to password requirements established in AFMAN 33-223.

4.2.1.7. Limit the capability to conduct privileged actions (i.e., loading new users, password management, modifying and patching system routines or files, examining memory locations, real-time monitoring of user activities, and initiating or executing privileged routines) to authorized personnel.

4.2.1.7.1. System administrators shall not have personal accounts with domain administrative privileges. For example, system administrators shall not check personal E-mails while logged in as an administrator. Sysadmin shall create regular user accounts for themselves to perform this function.

4.2.1.8. Implement auditing according to AFMAN 33-223 for information systems.

4.2.1.8.1. Establish an audit record capable of tracing network activity and actions to an individual user.

4.2.1.8.2. Ensure the audit mechanism records any event that attempts to change the security profile (e.g., access controls, security level of the subject, user password, etc.).

4.2.1.8.3. When technically feasible, ensure the information system aborts or suspends unauthorized user activity when detected, unless performing real-time analysis.

4.2.1.9. Generate output only within the central facility or at a remote station staffed with personnel cleared for the highest sensitivity level of information processed by the information system when the system does not have controls that limit output to authorized users.

4.2.1.10. Implement normal building and area entry controls (i.e., physical, administrative, and personnel security) at remote terminal sites when host systems have adequate internal access controls. Disable communications lines and take other necessary actions to protect information, systems, and resources when adequate internal controls do not exist.

4.2.1.11. Protect transmission of classified, sensitive, or a combination of classified and sensitive information according to AFI 33-201.

4.2.1.12. Protect emanations of classified, sensitive, or a combination of classified and sensitive information according to AFI 33-203.

4.2.2. Classified Processing. In addition to the security requirements listed in paragraph 4.1.2. and paragraph 4.2.1., the following security requirements apply. If conflicts develop, the following requirements take precedence:

4.2.2.1. Where the facility (building and room) plays a major role in providing security for information systems, establish procedures to notify wing IA office of impending changes to the facility.

4.2.2.2. Operate networks in a system high or dedicated security mode unless all network nodes are accredited for operation in the multilevel or partitioned security mode.

4.2.2.3. Use only SABI-approved devices and adhere to SABI configuration guidelines when connecting classified systems or networks to unclassified systems or networks (see paragraph 3.11. for additional SABI information).

4.2.2.4. Protect media according to AFI 31-401.

4.2.3. Ports, Protocols, and Services (PPS). The Air Force PPS matrix is an ongoing effort to provide policy for usage of known PPS on the Air Force enterprise. System developers and others responsible for bringing new information systems onto the Air Force enterprise shall ensure their systems conform to PPS outlined in the matrix. **NOTE:** The matrix does not list PPS usage for every Air Force information system, rather it provides overall policy for PPS use; should a conflict arise between the matrix and other operational guidance, or if a required PPS is not listed or is incorrect, contact HQ AFCA/WFPS. The matrix will be periodically updated as new information is presented. The PPS matrix is located at the Air Force IP web page (<https://private.afca.af.mil/ip>). **NOTE:** AFI 33-137, *Ports, Protocols, and Services (PPS) Management*, will contain Air Force PPS policy guidance when published.

**4.3. Portable Electronic Devices (PED).** PED is a generic title used to describe the myriad of small electronic items that are widely available. It is becoming difficult to differentiate between these electronic devices, as the trend is to combine capabilities and functions in various forms and format. PEDs include devices such as cellular telephones, laptop computers, handheld computers, bar code readers, personal digital assistants, etc. These all have wireless telecommunications capabilities that offer tremendous advantages for government users. When using wireless PEDs, operational security (OPSEC) and force protection should be considered prior to adoption of policy. OPSEC training and guidance can be obtained from the Interagency OPSEC Support Staff (<http://www.iooss.gov>). Any device that is lost or stolen should be reported to the ISSO or your supervisor (**NOTE:** See AFCA information protection homepage for additional security guidance). In addition to the information in paragraphs 4.1. and 4.2., the following additional requirements apply to PEDs.

4.3.1. Disable infrared (IR) port beaming capability. If the IR port is unable to be disabled, cover the IR port completely with metallic tape; ensure tape is not worn or torn.

4.3.2. Laptop Computers. There are documented occurrences where laptops taken to temporary duty (TDY) locations have been tampered with, both hardware tampering and modifications and software modifications. To mitigate the risk of compromised data and information systems, the following procedures should be considered:

4.3.2.1. Establish a dedicated laptop pool to support TDY travel and only use those laptops for that purpose.

4.3.2.2. Carefully consider prevention methods when transferring trip-specific information back to home stations. Examples are printing documents and scanning the documents on a computer on the network; transferring the information onto a portable hard-drive and performing examination and virus scanning on a stand-alone system prior to transferring to the network.

4.3.2.3. In cases where the laptops will be used in a secure facility, it may be best to leave the laptops in the secure facility at all times, rather than bringing them back and forth.

4.3.2.4. Laptops should not be left unattended. Maintain the same positive control over personal computer (PC) card devices (modem, FORTEZZA, etc.), portable printer devices, floppy disks, CD-ROMs, etc., that may accompany the laptop.

4.3.3. Personal Digital Assistants (PDA). Use of PDAs (e.g., Palm Pilot®, Cassiopeia®, Blackberry® devices, etc.) within the Air Force has increased significantly. When using wireless PEDs, OPSEC and force protection should be considered prior to adoption of any policy. OPSEC training and guidance can be obtained from the Interagency OPSEC Support Staff (<http://www.iooss.gov>). This family of devices offers personal productivity enhancements, particularly by making certain features of the desktop environment portable (e.g., Microsoft Outlook® contacts, notes, appointments, and E-mail); however, the use of some products and features introduces security risks to information systems and networks.

4.3.3.1. Usage.

4.3.3.1.1. Individuals may use PDAs to:

4.3.3.1.1.1. Process unclassified information from desktop workstations. This includes the following typical features: schedules, contact information, notes, E-mail, and other items.

4.3.3.1.1.2. Take notes, save information, or write E-mails when away from desktop workstations, whether down the hall or out of the country.

4.3.3.1.1.3. Synchronize information with desktop workstations.

4.3.3.1.2. Individuals cannot use PDAs to:

4.3.3.1.2.1. Process or maintain classified information. In the event classified information is processed or maintained on the PDA, the individual discovering the incident will notify the supervisor, security manager, servicing network control center or ISSO. The security manager will initiate actions required by AFI 31-401, *Information Security Program Management*, and prepare and coordinate an incident report with the commander and security forces squadron. The network control center, or network operations support center, will immediately take actions required by AFSSI 5020. The ISSO will confiscate PDAs that

have become contaminated with classified information. The DAA or DAA Representative determines the disposition of the contaminated PDA (destroy the affected PDA or hold until the PDA is sanitized according to AFFSI 5020.)

4.3.3.1.2.2. Connect or subscribe to commercial ISP for official E-mail services (e.g., Palmnet® wireless communications service). **NOTE:** Commercial ISP service (when required) can be authorized, provided transmission security (encryption) requirements outlined in paragraph 4.4.2.4. (this instruction) are strictly adhered to (see paragraph 4.1.1.7.). The use of commercial ISPs for official business is not encouraged due to the high operational risk posed by the possible collection of sensitive information.

4.3.3.1.2.3. Synchronize information across a network using a wireless connection. The configuration required to permit this functionality introduces unacceptable risks into a network--opening firewall ports and sending passwords in the clear. Evaluate exceptions to this restriction on a case-by-case basis and require DAA approval.

4.3.3.2. Only system administrators may download PDA applications. Software security restrictions, described in paragraph 3.3., apply to these devices.

4.3.3.2.1. The only authorized connection through a PDA modem is to an official Air Force remote access server (RAS) account protected by an authorized network control center firewall. Do not synchronize the PDA remotely by direct dial-in access to desktops.

4.3.3.2.2. Individuals must sign a PDA usage statement (**Attachment 3**) agreeing to the terms outlined in this instruction.

4.3.3.2.3. Additional security related information on PDAs is at the AFCA product evaluation web page (<https://private.afca.af.mil/prodeval>).

4.3.3.2.4. The following applies to handling and controlling PDAs:

4.3.3.2.4.1. Disable auto sync on the desktop application menu until needed. Once the PDA and computer have synchronized, turned off the auto-sync. Do not hot-sync outside existing firewall.

4.3.3.2.4.2. Password protect PDAs according to AFMAN 33-223. If the PDA is technically unable to use a password, increase physical access controls to prevent unauthorized access.

4.3.3.2.4.3. Turn off PDAs when not in use.

4.3.3.2.4.4. Purchase PDAs without audio recording capability, or ensure all microphones are disabled.

4.3.3.2.4.5. Disable video capture capability (if it exists).

4.3.3.2.4.6. Empty PDA cradles, when attached to a user PC, can be used to clone a PDA. Care should be taken to physically secure a cradle when not in use.

4.3.3.3. Include PDAs in the SSAA for the network. Ensure vulnerabilities associated with the PDAs are included in the threat and vulnerability assessment. Reflect the handling, controlling and usage of PDAs in the network security policy.

4.3.3.4. Connecting privately owned PDAs to the Air Force network is strongly discouraged. If individuals have a requirement to use a PDA on the Air Force network, they must request issuance

of a government-owned PDA. Privately owned PDAs will not be connected to the Air Force network without sufficient justification and the DAA approval. Justification must include mission requirements, government availability, and rationale of how duty position will be enhanced. Privately owned PDAs must have the same operating system as the government procures or supports. Include handling of privately owned PDAs and software in the SSAA. Individuals must sign a PDA usage statement ([Attachment 3](#)) agreeing to the terms outlined in this instruction.

4.3.3.5. Using PDAs in a classified environment is highly discouraged because of their infrared and similar recording capabilities.

4.3.3.5.1. On a case by case basis, PDAs may be authorized in a classified environment once an EMSEC inspection is accomplished. The DAA accepts the risk and vulnerabilities and updates the SSAA.

**4.4. Wireless Local Area Networks (WLAN).** (*NOTE:* WLAN devices, systems, services, and technologies that are integrated or connected to DoD networks are considered part of those networks, and shall comply with DoD Directive 8500.1 and be certified and accredited in accordance with DoD Instruction 5200.40. This includes systems for Joint use and Air Force systems that must interoperate directly with other Service or Coalition partner's networks.

4.4.1. WLANs (including wireless devices) are susceptible to interference and are easily jammed. Proposed WLAN solutions must be coordinated with the responsible spectrum manager prior to finalizing a technical solution and purchasing these products using AF Form 3215, **Information Technology/National Security Systems (IT/NSS) Requirements Document**, approval process. At non-US locations, coordinate with the MAJCOM Frequency Management Office to find out if Host Nation Approval (HNA) is required prior to operating any wireless LAN devices. Comply with AFI 33-118, *Radio Frequency (RF) Spectrum Management* and AFMAN 33-120, *Radio Frequency (RF) Spectrum Management*, and if nonlicensed WLAN interferes with another wireless solution on a base or vice-versa, the cognizant DAA will arbitrate. Vulnerabilities for WLANs are also applicable to wireless devices (i.e. wireless keyboards). WLAN Client devices and their WLAN hardware devices will be considered with respect to their capabilities to supply the required end-to-end encryption processing capacity and the capability for flexible technology upgrade to maintain interoperability and standardization at one base. Clearly define standards and publish WLAN security policies in the local network security policy. When using wireless PEDs, OPSEC and force protection should be considered prior to adoption of policy. OPSEC training and guidance can be obtained from the Interagency OPSEC Support Staff (<http://www.iooss.gov>). Apply the following security requirements to wireless solutions.

4.4.2. Existing WLANs are grandfathered until 1 October 2005, as long as they continue to meet current Air Force security policies and procedures.

4.4.2.1. All new WLANs will be in accordance with the standard design developed by the Combat Information Transport System (CITS) Program Office. WLAN solutions must meet the same C&A requirements as wired LAN solutions according to [Chapter 6](#). Application/Information System Program Management Offices must use the standard Air Force WLAN design during the development of a WLAN based information system. In addition Information System Program Management Office shall meet requirements outlined in AFI 33-103, *Requirements Development and Processing*, and base-level planning guidance found in AFI 33-104, *Base-Level Planning and Implementation*. It is the responsibility of the functional community to procure WLAN compliant

clients and ensure proper certification of the system in accordance with the Air Force Certification and Accreditation Process.

4.4.2.2. Engineer WLAN solutions to preclude backdoors into the Air Force enterprise network.

4.4.2.3. Configure wireless equipment for appropriate LAN security options. Commercial-off-the-shelf products typically arrive with factory default settings which may not offer LAN security.

4.4.2.4. Use encryption standards to protect information accordingly. Encrypt all radio frequency wireless networks according to AFI 33-201 (or DoD guidance, whichever is more restrictive). Comply with AFMAN 33-214, Volume 1, (*S*) *Emission Security Assessments (U)*, for WLANs.

4.4.2.5. Use NIST standard, FIPS Pub 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001, Triple data encryption standard encryption, or the advanced encryption standard for encryption of sensitive information.

4.4.2.6. The NCC will ensure that a user cannot enter a WLAN without strong authentication.

4.4.2.7. Conduct a risk analysis to determine the information intercept and monitoring vulnerabilities (e.g., electronic emanations, EMSEC, etc.), prior to implementing WLANs. Review all EMSEC assessments on all classified systems within the same building or within 20 meters of any components of the WLAN before beginning engineering, installation, or ordering the LAN.

4.4.2.8. Ensure that the administrators have the capability to audit or monitor the WLAN to detect intrusions. Intrusions are not always detected immediately. If logs are not available, it will be difficult to troubleshoot unauthorized access.

4.4.2.9. Remotely configure access points on the wired side of the WLAN configuration. This will prevent an intrusion on the wireless side from intercepting configuration information and changing the WLAN settings.

4.4.2.10. Simple Network Management Protocol is often used to remotely configure an access point. Change default community strings to prevent unauthorized configuration (read and write privileges to access point).

4.4.2.11. Ensure unused protocols are filtered at the access point. This will enhance the security and efficiency of the WLAN.

4.4.3. Consider the following characteristics and parameters of wireless solutions prior to the use of any wireless solution:

4.4.3.1. Wireless solutions may create backdoors into Air Force LANs. If a device receives information via a wireless technology and that device allows that information to be placed directly into the LAN via cable at the workstation level, then all perimeter and host-based security devices may have been bypassed.

4.4.3.2. When utilizing a wireless LAN solution the wireless LAN card's unique numeric identifier (MAC address) can be copied electronically (spoofed). It is important to ensure strong authentication (i.e., PKI or FIPS compliant device or SECNET 11). The user cannot rely totally on MAC address resolution as the only means for authentication.

4.4.3.3. Wireless Access Points (AP) shall be placed in accordance with the CITS Wireless Architecture System Design. Wireless APs shall be physically secured to prevent unauthorized access and tampering (**NOTE:** The NCC manages all wireless APs).

#### 4.5. Remote Access via Modem.

4.5.1. Centralize all modem management and remote access servers under the NCC. Do not use modems in any information system that is physically connected to the base network. Stand-alone PCs may use modems when approved by the DAA (i.e., Bulletin Board).

4.5.2. The security requirements (e.g., I&A, audit, etc.) of the local information system also apply to systems allowed to remotely access that information system.

4.5.3. Make sure that access tables, when used, remain current.

4.5.4. Prohibit the use of call-forwarding capabilities when using callback or dial-back technology.

4.5.5. Annotate remote access in the audit logs.

4.5.6. Do not publicize telephone numbers to anyone other than those with a need to know.

4.5.7. Employ methods for controlling access (e.g., virtual private network (VPN), callback, token generation, etc.) where the capability exists.

4.5.8. Dial-in hardware or software will disconnect sessions after 15 minutes of inactivity.

#### 4.6. Using Hardware or Software Not Owned by the Air Force.

4.6.1. Contractor-Owned. Contractor-owned or -operated hardware and software must meet all security requirements for government-owned hardware and software. AFI 31-601, *Industrial Security Program Management*, provides security policy and guidance relating to contractor actions involving classified information. DoD 5220.22-M, *National Industrial Security Program Operating Manual*, January 1995, applies to off-base contractor information systems and on-base contractor facilities when the Air Force does not have responsibility for industrial security inspections. If DoD 5220.22-M applies, Defense Investigative Service approval is mandatory before processing classified information. If the contractor must comply with this instruction instead of the manual, the Air Force must provide the contractor with specifications that establish contractor and Air Force responsibilities for security, including who should conduct the information system C&A and who the DAA is for the system. The program or project manager, contracting or procurement officer, and appropriate COMPUSEC personnel should jointly develop this guidance.

4.6.2. Other Service or Agency Owned. (**NOTE:** Where a lead service is other than the Air Force, some protection requirements may not be achievable). Develop an agreement before using equipment and facilities owned or operated by other services or agencies to ensure:

4.6.2.1. Air Force use of other services' or agencies' resources does not degrade the required security posture.

4.6.2.2. Mission-critical processing takes priority.

4.6.2.3. The lead service (in joint-service activities) identifies the DAA for the information system and determines security requirements for the information systems supporting the activity.

4.6.2.4. Requirements in this instruction, for the protection of Air Force information and information systems, are met.

4.6.3. Foreign Owned. Do not use foreign-owned or -operated (e.g., joint/coalition) information systems to process sensitive or classified information or for critical processing, unless required by international treaties or security agreements.

4.6.4. Privately Owned. Do not use privately owned information systems (i.e., hardware or software) to process classified information. Using privately owned hardware and software for government work is strongly discouraged; however, it may be used for processing unclassified and sensitive information with justification and DAA approval (see AFI 33-112, *Computer Systems Management*; and AFI 33-114, *Software Management*). Justification must include mission requirement, government availability, and rationale as to why privately owned information systems must be used. Approved privately owned information systems contaminated with classified information will be confiscated and sanitized. If unable to sanitize, the DAA will determine the disposition of the information system according to AFSSI 5020. Base approval on the following requirements:

4.6.4.1. The written approval specifies the conditions under which the information system operates. When using a privately owned information system for official work, the system must employ antivirus software, government-owned sensitive information must remain on removable media, and government-owned sensitive information must be marked and protected according to the sensitive category (e.g., Privacy Act, For Official Use Only [FOUO], etc.) program directives. This includes systems maintained at a residence, services accessed, and information transportation method(s) (modem, Telnet, Webmail, and/or physical media used).

4.6.5. Telecommuting. Prior to implementing a telecommuting program, consult AFI 36-8002, *Telecommuting Guidelines For Air Force Reservists and Their Supervisors*. This document is the approval authority for all requirements. Ensure vulnerabilities are assessed, with appropriate countermeasures employed, and documented in the certification and accreditation packages.

**4.7. Virtual Private Networks (VPN).** VPNs provide a secure encrypted means to transport data across the NIPRNET and within the Air Force enterprise.

4.7.1. All Air Force locations with an Air Force Service Delivery Point (SDP) shall bulk encrypt all AF.MIL to AF.MIL traffic before it traverses the NIPRNET. This configuration is known as the AF-VPN. AF-VPN traffic shall pass unencrypted through an Intrusion Detection System (IDS) to be examined before passing through the Base Information Protection (BIP) firewalls. All traffic shall pass through the AF-VPN from Air Force base to Air Force base. Submit requirements for other VPNs to HQ AFCA/ITL (Infostructure Architecture Council [IAC] Secretariat).

4.7.2. Strong auditing tools are required on both sides of the VPN tunnel. Document the auditing methodology in the appropriate SSAA(s).

4.7.3. Follow i-TRM recommended products list. Obtain interim approval to use other products from HQ USAF/XIC prior to implementation.

4.7.4. Security control requirements are based on the sensitivity of the information transmitted over the VPN. Use validated FIPS 140-2 cryptographic modules/devices.

4.7.5. Geographically Separated Units (GSU) requiring a protected connection to the NIPRNET will submit requirement for connection behind a Main Operating Base (MOB) to HQ AFCA CITS Lead Command.

4.7.6. VPN protection does not relieve programs from completing C&A, CoN, and CtO processes.

**4.8. Use of Multi-function Devices (MFD) on Unclassified Air Force Networks.** Some organizations that have purchased MFDs (combination network printer, copier, fax and scanner) may have been instructed to disable or disconnect the fax capability if the device was connected to the network. The full use of MFDs is authorized on unclassified networks under the following conditions:

4.8.1. The fax module must be configured to operate in 'Facsimile Class 1' mode and only allow connections to/from other fax machines. The ability to connect to a computer modem is not authorized. If available, bases should use the Telewall® Telecom Firewall or similar capability to secure MFD connections.

4.8.2. The MFD must comply with AFSSI 5020, *Remanence Security*, requirements for clearing/sanitizing storage media.

4.8.3. The MFD must be configured in accordance with the Multi-User Information Systems guidance outlined above.

4.8.4. The using organization must document the security features of the MFD in a request to the enclave Designated Approval Authority before connecting the device. Upon approval, update the SSAA.

**4.9. Information Assurance Requirements.** IA requirements shall be identified and included in the design, acquisition, installation, operation, upgrade, or replacement of all DoD information systems. IA controls, outlined in DoDI 8500.2 will be applied to all DoD information systems and must be addressed in all appropriate requirement documents.

## Chapter 5

### ACCESS TO INFORMATION SYSTEMS AND NETWORKS

**5.1. Access to Information Systems and Networks.** Grant access to information systems/networks, based on need-to-know, classification level of the information, security clearance, for official government business, special access (e.g., foreign national access, etc.), Information Technology [IT] (formerly Automated Information Systems (AIS) category designated requirements (e.g., local background investigation, national agency check, etc.), and qualifications. Users must have their User License (see paragraph [2.17.2.](#)). AFI 31-501 contains information on security clearances/background checks (or trustworthiness investigations) and IT position categories (**NOTE:** DoDI 8500.2 guidance will be followed—when more restrictive than AFI 31-501).

#### **5.2. Approving Foreign National Access and Use of Air Force Information Systems.**

5.2.1. *Access by foreign nationals to Air Force information systems, networks and enclaves is not authorized unless approved by a lieutenant general or equivalent.* It cannot be delegated. The approving authority is not required to approve or prohibit access on a case-by-case basis, rather he/she will determine, in general terms, whether foreign national access is or is not authorized. Approval or denial may apply to all foreign nationals or on a country-by-country basis. This determination will be documented in the SSAA. Additionally, if foreign nationals have been granted access to the information system, document it in the SSAA with the justification for the access, specific access restrictions placed on the individuals, and identify that they are an additional risk to the system. The appropriate approving authority for foreign national access and use of Air Force information systems/networks is listed in [Table 5.1](#). Before foreign nationals are authorized access and use of information systems:

5.2.1.1. The appropriate Foreign Disclosure Office authorizes access by foreign nationals to classified and controlled unclassified information in accordance with AFI 16-201, *Disclosure of Military Information to Foreign Governments and International Organizations*, the International Traffic in Arms Regulations (ITAR); the Export Administration Regulations (EAR); DoDD 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure*; DoDD 5400.7, *DoD Freedom of Information Act (FOIA) Program*; NDP-1, *National Policy and Procedures for the Disclosure of Classified Information to Foreign Governments and International Organizations*; DoDD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations* and DoDD 5230.20, *Visits, Assignments, and Exchanges of Foreign Nationals*. This includes information to which access or distribution limitations have been applied in accordance with national laws, policies, and regulations of the originating country. Ensure foreign disclosure officer (FDO) reviews and concurs that information to be accessed is required to support foreign national's duties and has been authorized for release to his or her government.

5.2.1.1.1. U.S. E-mail accounts of foreign nationals with access to U.S. systems will clearly identify in the E-mail address that the E-mail has originated from a foreign national. For example: Doe, John, Wing Commander, United Kingdom Exchange Officer, CENTAF/A6.

5.2.1.2. Validate that appropriate safeguards are in place and documented in SSAA. Ensure security measures employed adhere to DoD, Combatant Commanders/Services/Agencies, and local information assurance and system security policy and procedures.

5.2.1.3. Ensure individuals meet user licensing requirements (see paragraph [2.17.2.](#)).

5.2.2. Non-U.S. citizens may perform system or network administration, or other IT specialist duties, categorized as IT-I and IT-II (formerly known as AIS-I and AIS-II) positions. For those IT-I and IT-II positions that DoD policy identify as conditionally allowed, the information system DAA must ensure the following criteria from DoDI 8500.2, *Information Assurance (IA) Implementation*, is met before granting access:

**Table 5.1. Approving Authority for Foreign National Access and Use of USAF Information Systems, Networks, Enclaves, and the NIPRNET.**

If the system is a:	The Approving Authority is:
USAF functional system	HQ USAF 2-letter functional
HQ USAF-operated system	HQ USAF/CVA
SAF-operated system	SAF Assistant Secretary level
HQ USAF FOA or DRU functional system/enclave	HQ USAF /CVA
MAJCOM functional system/enclave	MAJCOM Commanders or Vice Commanders
MAJCOM FOA or DRU functional system/enclave	MAJCOM Commanders or Vice Commanders
Wing/Base functional/enclave	MAJCOM Commanders or Vice Commanders
NIPRNET	Appropriate lieutenant general or equivalent in organizational chain

5.2.2.1. Personnel security investigative levels for non-U.S. citizens must be equivalent to the investigative levels of U.S. citizens performing similar duties.

5.2.2.2. Non-U.S. citizens must be under the immediate supervision of a U.S. citizen.

5.2.3. Foreign nationals access to SIPRNET. The SIPRNET is a US-Only SECRET network. Foreign nationals will not be granted access to US-Only classified networks and terminals (e.g., US-Only Enclaves on SIPRNET) (see CJCSM 6510.01, *Defense-In-Depth: Information Assurance [IA] and Computer Network Defense [CND]*).

**5.3. Connection By Stand-Alone System.** Connection to an Air Force system/resource, by stand-alone systems or networks within a local enclave or through means other than the DISN (e.g., contractor’s facility, etc.) requires approval by the MAJCOM/CC or USAF/CVA. Coordinate requests through appropriate offices and include complete C&A documentation according to DITSCAP and this AFI.

**5.4. Accessing the SIPRNET.** For all Air Force systems accessing the DISN-SIPRNET get appropriate service (i.e., DISA) coordination and authorization before proceeding with combatant command coordination and/or Joint Staff approval.

**5.5. Requirements for Volunteers on the Network.**

5.5.1. Volunteers must meet the same requirements as Summer-Hire Employee in AFI 31-501. Volunteers are limited to IT-III (formerly known as AIS-III) level positions.

5.5.2. Volunteers must undergo User Licensing (see paragraph [2.17.2.](#)).

5.5.3. The SSAA will identify volunteers as having access to the information system and identify them as an additional risk to the system.

## Chapter 6

### CERTIFICATION AND ACCREDITATION

**6.1. Background.** The *Computer Security Act of 1987* established the requirement for every information system to be certified and accredited.

6.1.1. DoD 8510.1-M is the application manual that explains the step-by-step process on how to accomplish C&A using the DITSCAP. All systems will follow the DITSCAP.

6.1.2. Relationship of C&A, C4ISP, Network and MAJCOM Certificates.

6.1.2.1. DoD mandates the development of a C4ISP for all functional systems used within the DoD. The C4ISP is the program manager's planning document with the purpose of identifying support parameters necessary to ensure systems are fully supportable when placed into operation. The C4ISP addresses system-to-system interoperability, intelligence support, i-TRM compliance, security, sufficiency, and networkiness. To make networkiness a reality, the Air Force assesses systems and applications and issues a CoN based on the assessment of information contained in the C4ISP, SSAA, and other supporting documentation. Refer to DoDI 5000.2, *Operation of the Defense Acquisition System*, for further information about the acquisition process.

6.1.2.2. The C4ISP and SSAA are developed by the program or functional manager in parallel and both are assessed during the CoN and CtO processes. The CoN includes an in-depth review of a system's adherence to policy, procedures, and standards as it affects the security of the Air Force Enterprise Network.

6.1.2.3. AFCA issues a CoN stating the system has been evaluated and **does not** pose an unacceptable risk (in terms of networkiness) to the Air Force Enterprise Network. If a system is **not** networky, the capability will not be issued a CoN. Alternatively, a CoN may be issued with conditions. A CoN with Conditions places limits on the operation of the system (e.g., only behind a firewall or on its own server) or identifies actions that must be accomplished within a specified period of time (e.g., i-TRM migration plan to be provided within 90 days). Logically, a CoN without conditions remains when all conditions have been resolved (negating additional and unnecessary staffing of documentation).

6.1.2.4. The CoN is one input to the CtO process. The MAJCOM also considers MAJCOM unique issues such as the base's infrastructure, host nation support agreements, funding, training, etc. Then the MAJCOM CIO makes the decision to issue a CtO based on the information documented in the C4ISP, SSAA, port and protocol matrix, and other supporting documentation. Site DAAs then use the CoN and CtO to support local accreditation decisions. (**NOTE:** Issuance of a CoN does not automatically trigger a CtO issuance, nor does a CtO automatically trigger site DAA connection approval. Local DAAs may disapprove connectivity due to good cause regardless of CoN or CtO issuance.)

6.1.2.5. Further information on the Air Force C4ISP, CoN, and CtO processes can be found at the following web sites: <https://private.afca.af.mil/c4isp> or <https://private.afca.af.mil/con>. AFIs currently under development will contain additional information and guidance.

**6.2. Individual Roles and Responsibilities .** Key roles and responsibilities in the DITSCAP process include the DAA, DAA Representative, Certifier, Program Manager, User Representative, and the ISSO.

Some of these key roles are explained in **Chapter 2** of this instruction and additional information is contained in Chapter 8 of DoD 8510.1-M. There are numerous other personnel and agencies that support the C&A tasks. The number of participating organizations and their assignments will differ between programs based on the guidance set forth by the DAA, availability of resources, level of effort for certification, the security requirements, as well as the sensitivity and criticality of the system. It is equally important to identify their roles and responsibilities early on and include this information in the SSAA. In addition, the following information is provided as an overview of *typical* assignments of responsibilities to the various participants.

6.2.1. Designated Approving Authority (DAA). Official with the authority to formally assume the responsibility for operating a system or network at an acceptable level of risk. The DAA is also referred to as the accreditor and is the primary government official responsible for ensuring system security is applied to IT capabilities and networks within their purview. The DAA resides with the mission. The intent of this requirement is to ensure that the senior official whose mission might be adversely affected by security weaknesses in the information system is aware of and accepts the risks of operating the information system. See paragraph **2.13** for the DAA roles and responsibilities.

6.2.1.1. DAA Assignment.

**Table 6.1. DAA Assignment.**

<b>If the system is a:</b>	<b>Then, the DAA is:</b>	<b>And it may be delegated to:</b>
USAF functional system (Note 1)	HQ USAF 2-letter functional office	HQ USAF director-level functional office (Note 2)
HQ USAF FOA or DRU functional system/enclave	HQ USAF FOA OR DRU Commander	FOA or DRU director-level functional office
Special Access Program/ Special Access Required (SAP/ SAR) Systems	SAF/AA	Air Staff functional responsible for the security of the specific SAP/SAR program (Note 3)
MAJCOM functional system/ enclave (Notes 4 & 5)	MAJCOM Commander	MAJCOM director-level functional office
MAJCOM FOA or DRU functional system/enclave	MAJCOM FOA or DRU Commander	FOA or DRU director-level functional office
Wing/base functional system/ enclave (Note 5)	Host Wing Commander	Host Wing Vice Commander
Local Enclave (Note 6)	Commander of organization using the system	Functional office responsible for the system
Stand-alone System		

**NOTES:**

1. Functional systems (whether Air Force or MAJCOM unique) could be logistics systems, medical systems, personnel system, etc.; this also includes DoD and Joint Systems.

2. If the authority is delegated, those offices are the DAA for those functional systems from cradle to grave. For example, for the Integrated Logistics Systems-Supply, HQ USAF/IL could delegate DAA authority to HQ USAF/ILG, and for the Core Automated Maintenance System (CAMS), HQ USAF/ILM.
3. Further delegation may occur only with Administrative Assistant to the Secretary of the Air Force (SAF/AA) approval.
4. Includes all of their bases or sites owned by that MAJCOM. MAJCOM commanders reserve the right to assume DAA responsibility for a base enclave.
5. Includes the core services (E-mail, Internet services, video teleconferencing, etc.) boundary protection, network infrastructure (server farms, storage area networks routers, switches, and hubs, wireless access points, workstations, printers and network devices, etc.) regardless of ownership. When server consolidation happens, the base enclave then becomes a MAJCOM enclave.
6. Applies to closed systems not connected to any other enclave.

6.2.1.2. DAA Representative. To ease the burden of dealing with the day-to-day issues of information systems, the DAA may appoint a representative, in writing, to perform many of the duties. The DAA Representative identifies, addresses, and coordinates security C&A issues with the DAA and continuously keeps the DAA informed.

6.2.1.2.1. At the base level, normally the DAA Representative will be the host CSO.

6.2.1.2.2. A DAA Representative can sign site certification for functional systems and connection approvals for all systems. The DAA Representative can grant initial network access, as well as remove and restore network access when required in conjunction with various personnel actions.

**NOTE:** The DAA Representative can NOT accredit information systems (i.e., sign the SSAA for the DAA).

6.2.1.3. DAA Liability. It is imperative that the DAA understands the legal ramifications of signing the accreditation document. By signing the SSAA, the DAA verifies and assures the appropriate security measures, documentation, and the C&A process are implemented and maintained throughout the life cycle of the information systems.

6.2.1.3.1. When granting approval to operate, the DAA accepts the ultimate responsibility for the system's operation and officially declares:

6.2.1.3.1.1. The specified system adequately protects the information or resources.

6.2.1.3.1.2. Acceptance of the residual risks involved in operating the system.

6.2.1.3.1.3. After reasonable inquiry and analysis have been completed there are no known unacceptable risks of adverse ramifications to the mission (e.g., loss of life, etc.).

6.2.1.3.2. Maintain sufficient documentation to support the DAA's accreditation decision as well as to verify the implementation and operational maintenance of designated security measures or system safeguards.

6.2.1.4. DAA Training. DAAs need to familiarize themselves with responsibilities, directives, regulations, and laws applicable to C&A, before initiating the C&A process. See NSTISSI 4012, *National Training Standard for Designated Approving Authority (DAA)*.

6.2.2. Certifier. The Certifier is crucial to the success of the entire C&A effort. See paragraph 2.14. for the Certifier's roles and responsibilities. The Certifier should be a government employee, when possible, and should be trained to fill the position. See NSTISSI 4015, *National Training Standard for System Certifiers*.

6.2.3. Program Manager. The program manager coordinates all aspects of the system from initial concept through development, to implementation and system maintenance. The program manager performs roles listed in paragraph 2.12.

6.2.4. User Representative (User Rep). The User Rep is the liaison for the user community throughout the life cycle of the system. The User Rep defines the system's operational and functional requirements and is responsible for ensuring that the users' operational interest is maintained throughout system development, modification, integration, acquisition, and deployment. See DoD 8510.1-M, Chapter 8, for additional roles and responsibilities.

6.2.5. Information Systems Security Manager (ISSM). ISSMs establish and maintain COMPUSEC programs.

6.2.6. Information System Security Officer (ISSO). The ISSO assists in the development of the system security policy and ensures day-to-day compliance. During the Post-Accreditation Phase, they maintain the security posture and system accreditation. Additional roles are described in paragraph 2.14.1.

6.2.7. Other Roles.

6.2.7.1. Certification Team. Works for the Certifier to accomplish C&As according to the DITSCAP. Team members evaluate the technical and nontechnical features of the system to determine the level of protection provided and document their findings. Each member is responsible to the Certifier for the evaluations they perform and the documentation they submit. The composition and size of the team will depend on the size and complexity of the system. Ensure team members are independent of the system developers or project manager and the teams combined expertise spans the activities required.

6.2.7.2. System Security Working Group (SSWG). This group directs security tasks, and identifies and resolves security-related issues throughout the system life cycle according to AFPAM 63-1701 for systems under their purview. The group provides continuity among the system security policy, the system design, and the security engineering approach.

**6.3. System Security Authorization Agreement (SSAA).** The SSAA is a formal agreement among the DAA, the Certifier, user representative, and program manager. It contains information showing that the system meets the system security policy, all certification tasks are properly completed, the system is approved to operate, and a plan for maintaining the accreditation exists. For systems intended for classified or unclassified use, the SSAA must address the most restrictive requirements. Otherwise, separate SSAAs will be required.

6.3.1. SSAA Outline. Use the SSAA Outline and Detailed Description contained in DoD 8510.1-M, Appendix 1. List all items in the SSAA outline. For those items and appendices that do not apply, list

the SSAA outline number and title description, then insert nonapplicability (“N/A”) followed with a brief explanation stating the reason the appendix item is not applicable. See **Attachment 4** for a chart referencing SSAA tasks with specific paragraphs in DoD 8510.1-M.

6.3.1.1. In addition to applying DoD 8510.1-M Appendices A through R, the Air Force requires the following appendices:

6.3.1.1.1. Appendix S - Certificate of Networkiness/Networkiness Recommendation. A copy of the letters granting the certificate of networkiness and certificate to operate are listed in this appendix (if applicable).

6.3.1.1.2. Appendix T - Minimal Security Activity Checklists. See Appendix 2 of DoD 8510.1-M for the checklists. Complete the checklist for all levels.

6.3.1.1.3. Appendix U – Network Vulnerability Assessment Reports. A copy of the technical report produced by the vulnerability assessment application is included in this appendix. Use Internet Scanner or other approved application to perform the assessment.

6.3.1.1.4. Appendix V - Trusted Facility Manual (TFM). Use NCSC-TG-15, *A Guide to Understand Trusted Facility Management*, as a guide to assist with preparing the TFM.

6.3.1.1.5. Appendix W - Security Features User’s Guide (SFUG). Use NCSC-TG-026, *A Guide to Writing the Security Features User’s Guide for Trusted Systems*, as a guide to assist with preparing the SFUG. Software manuals and help files may also be used to meet the requirement of the SFUG.

6.3.1.2. MAJCOMs may require additional appendices to meet specific needs. Include all documentation that is relevant to the C&A process.

6.3.2. Automated Tools. DISA provides an automated tool to aid in the preparation of the SSAA and is available for downloading from <http://iase.disa.mil/ditscap/ssaa-v2.zip>.

6.3.3. Types of Accreditation. There are different types of accreditation depending on what is being certified.

6.3.3.1. Site Accreditation. Use to accredit the entire network for the base or site. It includes all local area networks, functional systems, and applications on that entire base or site network. Every base, station, GSU, etc. must have a site accreditation. This is also referred to as the network accreditation.

6.3.3.2. System Accreditation. Use to accredit functional systems and applications that are either not deployed to other locations, or are stand-alone systems.

6.3.3.3. Type Accreditation. Use to accredit functional systems and applications that are deployed to multiple locations, or application systems deployed without specific hardware to existing network resources.

6.3.3.3.1. Application certifications identify all baseline hardware used by a system when deployed to a typical location.

6.3.4. Certification Levels. The DITSCAP certification tasks must be performed at one of four certification levels. To determine the appropriate level of certification, the Certifier must analyze the system business functions, national, DoD, and agency security requirements, criticality of the system to the organization's mission, software products, computer infrastructure, data processed by the system,

and types of users. Considering this information, the Certifier determines the degree of confidentiality, integrity, availability, and accountability required for the system. Based on this analysis, the Certifier recommends a certification level: Level 1 – basic security review, Level 2 – minimum analysis, Level 3 – detailed analysis, or Level 4 – comprehensive analysis. The DITSCAP certification tasks must be performed at one of these four levels of certification.

6.3.4.1. The minimum certification level for stand-alone systems is Level 1.

6.3.4.1.1. Stand-alone systems may opt for the stand-alone template to complete the C&A for the information system (**NOTE:** Template is located on AFCA IP homepage).

6.3.4.1.2. Stand-alone systems containing FAX or modem hardware must be minimally certified at level 2 since they have the capability of connecting to other computers or systems.

6.3.4.2. All networked systems must be minimally certified at level 2 since they are connected to other computers or systems.

6.3.5. Accreditation Boundaries.

6.3.5.1. Networks. When accrediting a network, include the individual workstations in the network description providing these workstations contain similar hardware/software configuration. Check with the NCC for any local requirements concerning individual workstations and additional network accreditation requirements.

6.3.5.2. Systems. A system can be as small as a stand-alone workstation or as large as a complete network, with servers, router, hubs, workstations, etc. Software requires a platform (hardware) in order to operate. Certify the environment in which the software is operating. The software and hardware is accredited together as a system.

6.3.5.2.1. Cover all software and hardware in the SSAA. In some cases a single SSAA may include several systems. For example, if a piece of software or hardware (printer, PDA, biometrics device) is added to a network/workstation, etc., you do not have to accredit that specific software or hardware, but must add it to the existing SSAA. Update the existing SSAA, to include any new vulnerabilities or risks associated with adding the additional software or hardware. At a minimum, have the software scanned by certified agency (i.e., NOSC), using i-TRM approved tools and include the test results in the SSAA.

6.3.6. Security Test and Evaluation (ST&E). Use only i-TRM or DoD approved test tool software during ST&E. i-TRM recommended products are located at: <https://itrm.hq.af.mil>.

**6.4. Accreditation Decisions.** The decision to grant an accreditation or disapproval is based on the Certifier's recommendation and review of the SSAA. For systems that will utilize the Air Force network (defined as data passing between two or more bases), the DAA's accreditation decision may also include the security implications determined by a CoN, if available.

6.4.1. Accreditation. Accreditation is the formal declaration by the DAA that an information system or application is approved to operate in a particular security mode using a prescribed set of safeguards and controls; not to exceed three (3) years.

6.4.2. Interim Approval to Operate (IATO). An IATO may be issued by the DAA prior to the issuance of a CoN when the system requires an IATO in order to perform the testing required to complete the SSAA or when mission criticality mandates the system/application become operational and no other

capability exists to adequately perform the mission. The IATO is a temporary approval issued for the minimal period of time, up to one (1) year, necessary to meet all SSAA requirements and achieve accreditation.

6.4.3. Disapproval. If the decision is made to not authorize the system/application to operate, the DITSCAP process reverts to Phase 1 and the DAA, certifier, program manager, and user representative must agree to the proposed solutions to meet an acceptable level of risk. The decision must state the specific reason for denial and if possible, provide suggested solutions.

## 6.5. Site Certification.

6.5.1. Conduct site certification for systems and applications that have a CoN, a CtO, or have a type accreditation signed by the functional DAA upon its arrival at the site.

6.5.2. Site certification provides assurance that the operational location has implemented the required security measures. This evaluation ensures that the integration and operation of the system/application is in accordance with its certified design and operation concept, and poses an acceptable risk to the information being processed.

6.5.3. Site certification consists of:

6.5.3.1. Conducting the Site Accreditation Survey Checklist (See DoD 8510.1-M, Table AP2.T12).

6.5.3.2. Reviewing the local threats and vulnerabilities.

6.5.3.3. Testing the system/application installation and security configuration.

6.5.3.4. EMSEC certification completed, if required.

6.5.4. After considering the site certification evidence, the local Certifier documents the evidence in the SSAA. The DAA or DAA Representative then signs a letter verifying that the system/application is installed and operated according to the SSAA (**NOTE:** Site certification is not an acceptance of risk; it is a certification that the system will operate in accordance with CoN and CtO).

## 6.6. Reporting:

6.6.1. Report information system/application accreditation according to AFI 33-205.

6.6.2. Report information system/application vulnerabilities, security incidents, and virus attacks according to AFSSI 5021.

## 6.7. Information Collections, Records, and Forms or Information Management Tools (IMT).

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

6.7.2. Records: C&A records created by this publication should be maintained according to Air Force Web-RIMS RDS, Table 33-25, Rules 5.02 and 5.03. CoN and CtO are program records that should be maintained according to Air Force Web-RIMS RDS, Table 33-4, Rule 25 and Table 63-9, Rule 5.

6.7.3. Forms or IMTs: (Adopted and Prescribed).

6.7.3.1. Adopted Forms or IMTs: AF Form 847, **Recommendation for Change of Publication**, and AF Form 3215, **Information Technology/National Security Systems (IT/NSS) Requirements Document**.

6.7.3.2. Prescribed Forms or IMTs: No forms or IMTs are prescribed by this publication.

WILLIAM T. HOBBS, Lt. Gen, USAF  
DCS, Warfighting Integration

**Attachment 1****GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

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

Public Law 104-13, *The Paperwork Reduction Act of 1995*

Title 5 U.S. Code, Section 552a (Privacy Act)

Title 10 U.S. Code, Section 2224 (Defense Information Assurance Program)

FIPS Pubs 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001

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*

NDP-1, *National Policy and Procedures for the Disclosure of Classified Information to Foreign Governments and International Organizations*

NSTISSI 4012, *National Training Standard for Designated Approving Authority (DAA)*

NSTISSI 4015, *National Training Standard for System Certifiers*

NCSC-TG-15, *A Guide to Understanding Trusted Facility Management*

NCSC-TG-026, *A Guide to Writing the Security Features User's Guide for Trusted Systems*

CJCSM 6510.01, *Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)*

DoDI 5000.2, *Operation of the Defense Acquisition System*, May 12, 2003 (formerly DoD 5000.2-R)

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

DoDI 5200.40, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*, December 30, 1997

DoD 5220.22-M, *National Industrial Security Program Operating Manual*, January 1995, through Change 2, May 1 2000

DoD 5220.22-M Supplement 1, February 1995

DoDD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organization*, June 16, 1992

DoDD 5230.20, *Visits, Assignments, and Exchanges of Foreign Nationals*, August 12, 1998

DoDD 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure*, November 6, 1984 w/Change 1, August 18, 1995

DoD 5400.7-R/AF Sup 1, *Freedom of Information Act (FOIA) Program*, 24 June 2002

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

DoDD 8500.1, *Information Assurance*, October 24, 2002

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

DoD 8510.1-M, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual*, July 31, 2000

JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001 as amended through 14 August 2002

International Traffic in Arms Regulations (ITAR) (22 CFR Parts 120-130)

Export Administration Regulations (EAR)

AFPD 33-2, *Information Protection* (will become *Information Assurance*)

AFI 16-201, *Disclosure of Military Information to Foreign Governments and International Organizations* (to be published)

AFI 25-201, *Support Agreements Procedures*

AFI 31-401, *Information Security Program Management*

AFI 31-501, *Personnel Security Program Management*

AFI 31-601, *Industrial Security Program Management*

AFI 33-103, *Requirements Development and Processing*

AFI 33-104, *Base-Level Planning and Implementation*

AFI 33-112, *Computer Systems Management*

AFI 33-114, *Software Management*

AFI 33-115, Volume 1, *Network Management*

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

AFI 33-118, *Radio Frequency (RF) Spectrum Management*

AFI 33-137, (Draft) *Ports, Protocols, and Services (PPS) Management* (to be published)

AFI 33-201, *(FOUO) Communications Security (COMSEC)*

AFI 33-203, *Emission Security*

AFI 33-204, *Information Assurance Awareness Program*

AFI 33-205, *Information Protection Metrics and Measurements Program*

AFI 33-206, *Air Force Specialized Information Assurance Publications*

AFI 33-207, *Computer Security Assistance Program*

AFI 33-213, *DoD Public Key Infrastructure Management and Use*

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*

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

AFI 33-360, Volume 2, *Content Management Program-Information Management Tool (CMP-IMT)*

AFI 36-8002, *Telecommuting Guidelines For Air Force Reservists and Their Supervisors*

AFMAN 33-120, *Radio Frequency (RF) Spectrum Management*

AFMAN 33-214, Volume 1, *(S) Emission Security Assessments (U)*

AFMAN 33-214, Volume 2, *Emission Security Countermeasures Reviews*

AFMAN 33-223, *Identification and Authentication*

AFMAN 37-123, *Management of Records*

AFMAN 37-139 DELETED

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

AFPAM 63-1701, *Program Protection Planning*

AFSSI 5020, *Remanence Security* (will become AFMAN 33-224)

AFSSI 5021, *Time Compliance Network Order (TCNO) Management and Vulnerability and Incident Reporting*

WEB-RIMS, *Records Disposition Schedule (RDS)*

### ***Abbreviations and Acronyms***

**ADP**—Automated Data Processing

**AFCA**—Air Force Communications Agency

**AFCERT**—Air Force Computer Emergency Response Team

**AF-CIO**—Air Force Chief Information Officer

**AFI**—Air Force Instruction

**AFIWC**—Air Force Information Warfare Center

**AFMAN**—Air Force Manual

**AFMC**—Air Force Materiel Command

**AFPD**—Air Force Policy Directive

**AFSPC**—Air Force Space Command

**AFSSI**—Air Force Systems Security Instruction

**AIA**—Air Intelligence Agency

**AIS**—Automated Information System

**AP**—Access Points

**ASD/C3I**—Assistant Secretary of Defense for Command, Control, Communications and Intelligence

**ASD/NII**—Assistant Secretary of Defense for Networks and Information Integration (replaces the term ASD/C3I)

**ASIM**—Automated Security Incident Monitoring

**BIP**—Base Information Protection

**C4I**—Command, Control, Communications, Computers, and Intelligence

**C4ISP**—C4I Support Plan  
**C&A**—Certification and Accreditation  
**CAC**—Common Access Card  
**CC**—Common Criteria  
**CCB**—Configuration Control Board  
**CERT**—Computer Emergency Response Team  
**CITS**—Combat Information Transport System  
**CJCSI**—Chairman of the Joint Chiefs of Staff Instruction  
**COMPUSEC**—Computer Security  
**COMSEC**—Communications Security  
**CoN**—Certificate of Networthiness  
**CSO**—Communications and Information Systems Officer  
**CtO**—Certificate to Operate  
**DAA**—Designated Approving Authority  
**DAC**—Discretionary Access Control  
**DISA**—Defense Information Systems Agency  
**DISN**—Defense Information Systems Network  
**DITSCAP**—DoD Information Technology Security Certification and Accreditation Process  
**DoD**—Department of Defense  
**DoDD**—Department of Defense Directive  
**DRU**—Direct Reporting Unit  
**DSAWG**—DISN Security Accreditation Working Group  
**EAL**—Evaluation Assurance Level  
**EAR**—Export Administration Regulations  
**EMSEC**—Emission Security  
**FDO**—Foreign Disclosure Office  
**FIPS**—Federal Information Processing Standards  
**FOA**—Field Operating Agency  
**FOUO**—For Official Use Only  
**FTP**—File Transfer Protocol  
**GIAP**—GIG Interconnection Approval Process  
**GIG**—Global Information Grid

**GSU**—Geographically Separated Units  
**IA**—Information Assurance  
**IATO**—Interim Approval to Operate  
**IDS**—Intrusion Detection Service  
**I&A**—Identification and Authentication  
**IPO**—Information Protection Operations  
**IR**—Infrared  
**ISP**—Internet Service Provider  
**ISSM**—Information System Security Manager  
**ISSO**—Information System Security Officer  
**IT**—Information Technology  
**ITAR**—International Traffic in Arms Regulations  
**i-TRM**—Infostructure Technical Reference Model  
**JP**—Joint Publication  
**MAC**—Media Access Control  
**MAJCOM**—Major Command  
**MFD**—Multi-function Devices  
**NATO**—North Atlantic Treaty Organization  
**NCC**—Network Control Center  
**NCSC**—National Computer Security Center  
**NIAP**—National Information Assurance Partnership  
**NIPRNET**—Non-Secure Internet Protocol Router Network  
**NIST**—National Institute of Standards and Technology  
**NOSC**—Network Operations and Security Center  
**NSA**—National Security Agency  
**OMB**—Office of Management and Budget  
**OPSEC**—Operational Security  
**PC**—Personal Computer  
**PDA**—Personal Digital Assistants  
**PED**—Personal Electronic Device  
**PKI**—Public Key Infrastructure  
**P.L.**—Public Law

**POC**—Point of Contact

**PPS**—Ports, Protocol, and Services

**RAS**—Remote Access Server

**RDS**—Records Disposition Schedule

**SABI**—Secret and Below Interoperability

**SAF**—Secretary of the Air Force

**SAF/AA**—Administrative Assistant to the Secretary of the Air Force

**SAP/SAR**—Special Access Program/Special Access Required

**SCAO**—SIPRNET Connection Approval Office

**SCD**—Systems Compliance Database

**SCI**—Sensitive Compartmented Information

**SDP**—Service Delivery Point

**SFUG**—Security Feature User's Guide

**SIPRNET**—Secret Internet Protocol Router Network

**SSAA**—System Security Authorization Agreement

**SSWG**—System Security Working Group

**ST&E**—Security Test and Evaluation

**TCNO**—Time Compliance Network Order

**TFM**—Trusted Facility Manual

**URL**—Uniform Resource Locator

**VPN**—Virtual Private Network

**WLAN**—Wireless Local Area Network

**WM**—Workgroup Manager

### *Terms*

**Accountability**—Process of tracing information systems activities to a responsible source.

**Accreditation**—Formal declaration by a DAA that an information system 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 (AIS)**—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 computer, a central computer system with remote terminals (e.g., mainframe), a LAN, or a Wide Area Network (WAN).

**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.

**Category**—A grouping of classified or sensitive information to which an additional restrictive label is applied to signify that personnel are granted access to the information only if they have access approval (e.g., formal access approval). Examples include proprietary, FOUO, Privacy Act, North Atlantic Treaty Organization (NATO), and compartmented 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.

**Certifier**—Individual responsible for making a technical judgment of the information systems compliance with stated security requirements and requesting approval to operate from the DAA.

**Common Criteria**—The International Common Criteria for Information Technology Security Evaluation (CC) defines general concepts and principles of information technology (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-Based Security**—Security for the information system is provided through the use of automated security features.

**Computer Network**—The constituent element of an enclave responsible for connecting computing environments by providing short-haul data transport capabilities, such as local or campus area networks, or long-haul data transport capabilities, such as operational, metropolitan or 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.

**Controlled Unclassified Information**—Information that is not classified but has some restrictions placed on it, such as export controls or exemption from the Freedom of Information Act.

**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. (**NOTE:** There are two divisions of control: management [policy, objectives, and criteria class] and internal [security requirements, mechanisms, and rules]. DoDD 8000.1, *Management of DoD Information Resources and Information Technology*, 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.

**Designated Approving Authority (DAA)**—Official with the authority to formally assume responsibility for operating an information system or network within a specified environment.

**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 mission assurance category 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 as defined in OMB A-130. 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 local area networks and the applications they host, backbone networks, and data processing centers.

**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 (Common Criteria (IS 15408)) 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 Nationals**—All individuals who are non-U.S. citizens including U.S. military personnel, DoD civilian employees and contractors.

**Formal Access Approval**—Documented approval by a data owner to allow access to a particular category of information.

**Functional System**—A specific system used, owned, operated, and maintained by a functional community

**Global Information Grid (GIG)**—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 National Security Systems (NSS) as defined in section 5142 of the Clinger-Cohen Act of 1996 (reference (f)). 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.

**IA Product**—Product or technology whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control or nonrepudiation of data); correct known vulnerabilities; and/or provide layered defense against various categories of nonauthorized or malicious

penetrations of information systems or networks. Examples include such products as data/network encryptors, firewalls, and intrusion detection devices.

**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.

**Information**—1.--Data derived from observing phenomena and the instructions required to convert that data into meaningful information. (**NOTE:** Includes: operating system information such as system parameter settings, password files, audit data, etc.) 2. (DoD) Facts, data, or instructions in any medium or form. (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 information system (IS) and network security intrusions. The NCC conducts IPO employing hardware and software tools to enhance the security of their networks

**Information System**—1. Any telecommunications and/or computer-related equipment or interconnected system or subsystems of equipment used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice, and/or data, including software, firmware, and hardware. (**NOTE:** This includes automated information systems.) 2. (DoD) The entire infrastructure, organization, and components that collect, process, store, transmit, display, disseminate, and act on information. (JP 1-02).

**Information Systems Security Manager (ISSM)**—Principal advisor on computer security matters to DAA. (**NOTE:** DoDI 8500.2 IA Manager (IAM). The individual responsible for the information assurance program of a DoD information system or organization. While the term IAM is favored within the Department of Defense, it may be used interchangeably with the IA title Information Systems Security Manager (ISSM)).

**Information Systems Security Officer (ISSO)**—Official who manages the COMPUSEC program for an information system assigned to him or her by the ISSM; including monitoring information system activities, and ensuring that the information system is operated, maintained, and disposed of according to security policies and practices. (**NOTE:** DoDI 8500.2 IA Officer (IAO). An individual responsible to the IAM for ensuring that the appropriate operational IA posture is maintained for a DoD information system or organization. While the term IAO is favored within the Department of Defense, it may be used interchangeably with other IA titles (e.g., Information Systems Security Officer, Information Systems Security Custodian, Network Security Officer, or Terminal Area Security Officer).

**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 (IT)**—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.

**IT Position Category**—Applicable to unclassified DoD information systems, 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 (reference (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 (ADP) 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 information system.

**Mission Assurance Category**—Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. DoD has three defined mission assurance categories:

**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.

**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.

**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.

**Network Security Policy**—Overall policy that is developed for the network. This policy regulates how sensitive and classified information is managed, protected, and distributed on the network. It also includes boundary protection, rules of engagement, methods of protection.

**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.

**Periods Processing**—Processing of various levels of classified and unclassified information at distinctly different times. (**NOTE:** Under periods processing, the information system [operating in dedicated security mode] is purged of all information from one processing period before transitioning to the next when there are different users with different authorizations.)

**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 information system. (Synonymous with Single Manager or Project Manager.)

**Safeguards**—Protective measures and controls prescribed to meet the security requirements of an information system. (**NOTE:** 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; media access control (MAC); discretionary access control (DAC); object reuse; or audit. Security features are a subset of information system 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 (Privacy Act), 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. (**NOTE:** Systems that are not national security systems, but contain sensitive information are subject to be protected in accordance with the requirements of the Computer Security Act of 1987 [P.L. 100-235].)

**Site Certification**—Provides assurance that the operational location has implemented the required security measures. This evaluation ensures that the integration and operation of the system is in accordance with the SSAA and a review of the local environment (threats/vulnerabilities).

**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 information system) and the threat.

**Stand-Alone System**—An information system 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 PC with removable storage media such as a floppy disk).

**Standard System**—Two or more substantively similar information systems developed for the purpose of fielding multiple copies in support of a mission, within or across MAJCOM or service lines, or DoD-wide.

**Strong Authentication**—Two of the three approved methods of authentication: something you know (password), something you have (token), or something you are (biometric).

**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.

**System Security Policy**—Set of laws, rules, and practices that regulate how sensitive and classified information is managed, protected, and distributed by an information system. (**NOTE:** It interprets

regulatory [e.g., DoDD 8500.1, AFPD 33-2, AFI 33-202, etc.] and operational requirements for a particular system and states how that system will satisfy those requirements. All systems or networks, regardless of their sensitivity, criticality, or life-cycle phase, will have a system security policy.).

**Tampering**—Unauthorized modification that alters the proper functioning of information system security equipment.

**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 information system by direct connections (e.g., via terminals) or indirect connections.

**Vulnerability**—1. Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited. 2. (DoD) 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. (JP 1-02) 3. (DoD) 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)

**Workgroup Manager (WM)**—A duty supporting a functional community (e.g., workcenters, flights, squadrons, or organizations) and is the first line of help customers contact to resolve problems.

## Attachment 2

### MOBILE CODE WAIVER PROCESS

#### **A2.1. Waiver Process for Use of Category 1 Unsigned Mobile Code in Situations Considered Critical to the Performance of a Mission:**

A2.1.1. Within the body of the waiver, detail the program/project mission, specify the justification for the requested mobile code technology, including explanation for why the program/project requires the requested mobile code technology. Identify whether lower risk category (i.e., 2 or 3) technologies were considered and provide an analysis why lower risk categories cannot meet the program/project's mission. Include a risk and vulnerabilities analysis for using the requested mobile code, and category currently assigned to the mobile code. Detail the security configurations, and other methods to mitigate the risk and vulnerabilities from the analysis.

A2.1.2. The waiver shall stipulate in detail the use of a mobile code product to include: the physical location and classification of data residing on the system, including any external network and system interfaces.

A2.1.3. Identify the mechanisms to be used for trusted source and assured channel.

#### **A2.2. Waiver Process for Category 2 Mobile Code Not Obtained from Trusted Sources over Assured Channels.**

A2.2.1. Within the body of the waiver, detail the program/project mission, specify the justification for the requested mobile code technology, including explanation for why the program/project requires the requested mobile code technology. Identify the specific mobile code technology to be used, with a description of the operation environment including the physical location, classification of data residing on the system, and external network and system interfaces.

A2.2.2. For category 2 Mobile Code not obtained from a trusted source over an assured channel, a request for using category 2 Mobile Code shall be included in the waiver to include a risk and vulnerability assessment identifying risk mitigation's strategies to be used for malicious mobile code.

A2.2.3. Identify the mechanisms to be used for trusted source and assured channel.

**A2.3. Use of Commercial PKI Certificates.** Until DoD PKI code signing certificates are available, commercial code signing certificates will be used as an alternate for DoD PKI code signing certificates. Specify the justification for use of commercial code signing certificates in the waiver request.

**A2.4. Submitting Waivers.** Submit requests for waivers through a MAJCOM/SC, FOA/SC, DRU/SC to HQ USAF/ILC.

**Attachment 3****EXAMPLE OF PDA USER AGREEMENT**

MEMORANDUM FOR

FROM: \_\_\_\_\_  
(Rank, Name, Office Symbol)

Date: \_\_\_\_\_

Subject: Agreement to Use DAA-Approved Privately Owned Personal Digital Assistants (PDA) on the Air Force Enterprise Network

1. My signature below indicates I understand that my privately owned PDA, which is a similar type PDA to the approved government PDAs, has been approved for use by the DAA of the system I am connecting to. In addition to the requirements in AFI 33-202, *Network and Computer Security*, I agree to all the terms, actions, and conditions contained in this letter.

2. I will:

- a. Register my PDA with my local equipment custodian for local accountability.
- b. Maintain a password on my PDA according to the system security policy.
- c. Only use my PDA to process unclassified, non-Privacy Act information.
- d. Maintain the same antivirus software, security standards, and other operational requirements as the government issued PDAs and pay for what is required.
- e. Not connect or subscribe to commercial Internet service provider for official E-mail services.
- f. Not synchronize information across the Air Force network using a wireless connection.
- g. Physically disable any built-in wireless connectivity capability, including infrared.
- h. Surrender my PDA (with no reimbursement) if classified information contaminates my PDA.
- i. Report any software abnormalities to the ISSO.
- j. Not load any software on my PDA without prior authorization.
- k. Submit my personal PDA, prior to leaving my current duty assignment, for removal of all sensitive information.
- l. Only connect my PDA to the network or system approved by the DAA.
- m. Consent to monitoring of my PDA, since it is connected to a system that is subject to being monitored.

3. I understand my PDA is subject to being audited at any time to determine if my PDA contains Privacy Act or classified information.

4. I understand that the process for sanitizing sensitive and classified information from my PDA may result in its destruction and I waive any and all claims for reimbursement for any damage or destruction.

5. I understand the Help Desk will assist me with all PC-related problems but repair of my PDA is my responsibility.

6. I understand that if at any time I fail to meet the conditions stated above, I will be required to remove my PDA from connection within the Air Force protected enclave and submit it for data sanitization.

7. I understand the Air Force does not assume any liability for my PDA, regardless of circumstance. I understand that all data entered on my PDA while performing government business becomes the property of the U.S. Government.

8. Device information:

a. Make & Model: \_\_\_\_\_

b. Serial number: \_\_\_\_\_

c. Operating system: \_\_\_\_\_

d. Installed software: \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

9. I can be contacted at: \_\_\_\_\_

(phone number and office symbol)

Signature: \_\_\_\_\_

Signature Block: \_\_\_\_\_

File:

1. Maintain original copy with the ISSO

2. Provide one copy to the individual

## Attachment 4

## DITSCAP - C&amp;A TASKS

A4.1. [Table A4.1.](#) is taken from DoDI 5200.40.

**Table A4.1. DITSCAP - C&A Tasks.**

Tasks	Para #	Output / Product
<b>Phase I: Definition</b>	<b>Chapter 3</b>	
<b>Preparation</b>	C3.3.2.	
1-1. Review documentation	C3.4.1.	None
<b>Registration</b>	C3.3.3.	
1-2. Prepare Mission Description and System Identification	C3.4.2.	SSAA, Section 1
1-3. Register System	C3.4.3.	Functional Systems are registered in the SCD
1-4. Prepare Environment & Threat Description	C3.4.4.	SSAA, Section 2
1-5. Determine System Security Requirements	C3.4.5.	SSAA, Section 4
1-6. Prepare System Security Architecture Description	C3.4.6.	SSAA, Section 3
1-7. Identify Organizations & Resources	C3.4.7.	SSAA, Section 5
1-8. Tailor DITSCAP/Prepare DITSCAP Plan	C3.4.8.	SSAA, Section 6
1-9. Draft the SSAA	C3.4.9.	Completed draft SSAA Document
<b>Negotiation</b>	C3.3.4.	
1-10. Conduct Certification Requirements Review	C3.4.10.	None
1-11. Establish Agreement on Level of Effort and Schedule	C3.4.11.	None
1-12. Approve Phase I SSAA	C3.4.12.	Approved SSAA
<b>Phase II: Verification</b>	<b>Chapter 4</b>	
<b>SSAA Refinement</b>	C4.2.1.	If necessary, update SSAA
<b>Systems Integration and Development</b>	C4.2.2.	None
<b>Initial Certification Analysis</b>	C4.2.3.	
2-1. System Architecture Analysis	C4.3.2.	Minimal Security Activity Checklist Table AP2.T1 and Summary Report (Table C4.T2)
2-2. Software, Hardware and Firmware Design Analysis	C4.3.3.	Minimal Security Activity Checklist Table AP2.T2 and Summary Report (Table C4.T2)
2-3. Network Connection Rule Compliance	C4.3.4.	Minimal Security Activity Checklist Table AP2.T3 and Summary Report (Table C4.T2)
2-4. Integrity Analysis of Integrated Products	C4.3.5.	Minimal Security Activity Checklist Table AP2.T4 and Summary Report (Table C4.T2)
2-5. Life Cycle Management Analysis	C4.3.6.	Minimal Security Activity Checklist Table AP2.T5 and Summary Report (Table C4.T2)
2-6. Security Requirements Validation Procedures	C4.3.7.	Customized Minimum Security Checklist Table AP2.T6 Test Plans and Procedures
2-7. Vulnerability Assessment	C4.3.8.	Vulnerability Assessment Report
<b>Phase III: Validation</b>	<b>Chapter 5</b>	
<b>SSAA Refinement</b>	C5.2.1.	If necessary, update SSAA
<b>Certification Evaluation of Integrated System</b>	C5.2.2.	
3-1. Security Test & Evaluation (ST&E)	C5.3.2.	Minimal Security Activity Checklist Table AP2.T7 and Summary Report (Table C5.T2)

Tasks	Para #	Output / Product
3-2. Penetration Testing	C5.3.3.	Minimal Security Activity Checklist Table AP2.T8 and Summary Report (Table C5.T2)
3-3. TEMPEST and RED-BLACK Verification	C5.3.4.	Minimal Security Activity Checklist Table AP2.T9 and Summary Report (Table C5.T2)
3-4. COMSEC Compliance Evaluation	C5.3.5.	Minimal Security Activity Checklist Table AP2.T10 and Summary Report (Table C5.T2)
3-5. System Management Analysis	C5.3.6.	Minimal Security Activity Checklist Table AP2.T11 and Summary Report (Table C5.T2)
3-6. Site Accreditation Evaluation	C5.3.7.	Minimal Security Activity Checklist Table AP2.T12 and Summary Report (Table C5.T2)
3-7. Contingency Plan Evaluation	C5.3.8.	Minimal Security Activity Checklist Table AP2.T13 and Summary Report (Table C5.T2)
3-8. Risk Management Review	C5.3.9.	Minimal Security Activity Checklist Table AP2.T14 and Summary Report (Table C5.T2)
<b>Recommendation to DAA</b>	C5.2.3.	<b>Certifier's Recommendation</b>
<b>Senior Level SSAA Review</b>	<i>note 1</i>	<b>Network Risk Assessment Report</b>
<b>DAA Accreditation Decision (note2)</b>	C5.2.4.	<b>DAA's Accreditation Letter</b>
Phase IV: Post-accreditation	<b>Chapter 6</b>	
<b>System and Security Operation</b>	C6.2.1.	
4-1. SSAA Maintenance	C6.3.2.	<b>A Revised SSAA</b>
4-2. Physical, Personnel and Management Control Review	C6.3.3.	<b>Summary Report (Table C6.T3)</b>
4-3. TEMPEST Evaluation	C6.3.4.	<b>Summary Report (Table C6.T3)</b>
4-4. COMSEC Compliance Evaluation	C6.3.5.	<b>Summary Report (Table C6.T3)</b>
4-5. Contingency Plan Maintenance	C6.3.6.	<b>Summary Report (Table C6.T3)</b>
4-6. Configuration Management	C6.3.7.	<b>Summary Report (Table C6.T3)</b>
4-7. Risk Management Review	C6.3.8.	<b>Summary Report (Table C6.T3)</b>
<b>Compliance Validation</b>	C6.2.2.	
4-8. Compliance Validation	C6.3.9.	<b>Summary Report (Table C6.T3)</b>

**NOTES:**

1. Systems and applications that do not require a CoN or CtO process still require a Risk Assessment performed on them.
2. DAA's decision to accredit is based on the Certifier's recommendation. The certifier's recommendation will be based on the SSAA, and for site certifications, the CoN and CtO (if applicable).

## Attachment 5

### INTERIM CHANGE 2004-1 TO AIR FORCE INSTRUCTION (AFI) 33-202, NETWORK AND COMPUTER SECURITY

17 JUNE 2004

This Air Force instruction (AFI) implements the computer security (COMPUSEC) portion of Air Force Policy Directive (AFPD) 33-2, *Information Protection* (will become *Information Assurance*), and establishes Air Force COMPUSEC requirements for information protection compliance with Public Law (P.L.) 100-235, *Computer Security Act of 1987*; 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 U.S. Code, Section 2224 (Defense Information Assurance Program), Department of Defense Directive (DoDD) 8500.1, *Information Assurance (IA)*, October 24, 2002; Department of Defense Instruction (DoDI) 8500.2, *Information Assurance (IA) Implementation*, February 6, 2003; DoDI 5200.40, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*, December 30, 1997; Department of Defense (DoD) 8510.1-M, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual*, July 31, 2000; and CJCSM 6510.01, *Defense-In-Depth: Information Assurance [IA] and Computer Network Defense [CND]*. The Uniform Code of Military Justice applies to personnel who violate the specific prohibitions and requirements of this instruction. This instruction gives the directive requirements for the COMPUSEC component of the Information Assurance (IA) discipline 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. 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. Additional instructions and manuals are listed on the Air Force Publishing web site at Uniform Resource Locator (URL): <http://www.e-publishing.af.mil> under Electronic Publications. Air Force Directory (AFDIR) 33-303, *Compendium of Communications and Information Terminology*, explains other terms. Direct questions or comments on the contents of this instruction, through appropriate command channels, to Headquarters Air Force Communications Agency (HQ AFCA/WFP), 203 W. Losey Street, Room 2200, Scott AFB IL 62225-5222. Refer recommended changes and conflicts between this and other publications to HQ AFCA/ITXD, 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, through appropriate channels, using AF Form 847, **Recommendation for Change of Publication**. Provide an information copy to HQ AFCA/WFP. Send any supplements to this publication to HQ AFCA/WFP for review, coordination, and approval prior to publication. Provide a copy of each final supplement to HQ AFCA/ITXD. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records*, and disposed of in accordance with Air Force Web-RIMS, *Records Disposition Schedule (RDS)* located at <https://webrims.amc.af.mil/rds/index.cfm>. Public Law 104-13, *The Paperwork Reduction Act of 1995* and AFI 33-360, Volume 2, *Content Management Program-Information Management Tool (CMP-IMT)*, affect this publication. 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 REVISIONS

This update incorporates interim change (IC) 2004-1. The revision brings the foreign national administrator policy and the certifier criteria in-line with DoD policy. The other changes are administrative in nature and do not reflect policy change. A “[” indicates revised material since the last edition.

4.2.3. Ports, Protocols, and Services (PPS). The Air Force PPS matrix is an ongoing effort to provide policy for usage of known PPS on the Air Force enterprise. System developers and others responsible for bringing new information systems onto the Air Force enterprise shall ensure their systems conform to PPS outlined in the matrix. **NOTE:** The matrix does not list PPS usage for every Air Force information system, rather it provides overall policy for PPS use; should a conflict arise between the matrix and other operational guidance, or if a required PPS is not listed or is incorrect, contact HQ AFCA/WFPS. The matrix will be periodically updated as new information is presented. The PPS matrix is located at the Air Force IP web page (<https://private.afca.af.mil/ip>). **NOTE:** AFI 33-137, *Ports, Protocols, and Services (PPS) Management*, will contain Air Force PPS policy guidance when published.

4.3.3.2.3. Additional security related information on PDAs is at the AFCA product evaluation web page (<https://private.afca.af.mil/prodeval>).

4.7.1. All Air Force locations with an Air Force Service Delivery Point (SDP) shall bulk encrypt all AF.MIL to AF.MIL traffic before it traverses the NIPRNET. This configuration is known as the AF-VPN. AF-VPN traffic shall pass unencrypted through an Intrusion Detection System (IDS) to be examined before passing through the Base Information Protection (BIP) firewalls. All traffic shall pass through the AF-VPN from Air Force base to Air Force base. Submit requirements for other VPNs to HQ AFCA/ITL (Infostructure Architecture Council [IAC] Secretariat).

5.2.2. Non-U.S. citizens may perform system or network administration, or other IT specialist duties, categorized as IT-I and IT-II (formerly known as AIS-I and AIS-II) positions. For those IT-I and IT-II positions that DoD policy identify as conditionally allowed, the information system DAA must ensure the following criteria from DoDI 8500.2, *Information Assurance (IA) Implementation*, is met before granting access:

5.2.2.1. Personnel security investigative levels for non-U.S. citizens must be equivalent to the investigative levels of U.S. citizens performing similar duties.

5.2.2.2. Non-U.S. citizens must be under the immediate supervision of a U.S. citizen.

5.2.3. Foreign nationals access to SIPRNET. The SIPRNET is a US-Only SECRET network. Foreign nationals will not be granted access to US-Only classified networks and terminals (e.g., US-Only Enclaves on SIPRNET) (see CJCSM 6510.01, *Defense-In-Depth: Information Assurance [IA] and Computer Network Defense [CND]*).

6.1.2.5. Further information on the Air Force C4ISP, CoN, and CtO processes can be found at the following web sites: <https://private.afca.af.mil/c4isp> or <https://private.afca.af.mil/con>. AFIs currently under development will contain additional information and guidance.

6.2.2. Certifier. The Certifier is crucial to the success of the entire C&A effort. See paragraph 2.14. for the Certifier’s roles and responsibilities. The Certifier should be a government employee, when possible, and should be trained to fill the position. See NSTISSI 4015, *National Training Standard for System Certifiers*.

6.7.2. Records: C&A records created by this publication should be maintained according to Air Force Web-RIMS RDS, Table 33-25, Rules 5.02 and 5.03. CoN and CtO are program records that should be maintained according to Air Force Web-RIMS RDS, Table 33-4, Rule 25 and Table 63-9, Rule 5.

**Attachment 1****GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

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

Public Law 104-13, *The Paperwork Reduction Act of 1995*

Title 5 U.S. Code, Section 552a (Privacy Act)

Title 10 U.S. Code, Section 2224 (Defense Information Assurance Program)

FIPS Pubs 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001

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*

NDP-1, *National Policy and Procedures for the Disclosure of Classified Information to Foreign Governments and International Organizations*

NSTISSI 4012, *National Training Standard for Designated Approving Authority (DAA)*

NSTISSI 4015, *National Training Standard for System Certifiers*

NCSC-TG-15, *A Guide to Understanding Trusted Facility Management*

NCSC-TG-026, *A Guide to Writing the Security Features User's Guide for Trusted Systems*

CJCSM 6510.01, *Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)*

DoDI 5000.2, *Operation of the Defense Acquisition System*, May 12, 2003 (formerly DoD 5000.2-R)

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

DoDI 5200.40, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*, December 30, 1997

DoD 5220.22-M, *National Industrial Security Program Operating Manual*, January 1995, through Change 2, May 1 2000

DoD 5220.22-M Supplement 1, February 1995

DoDD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organization*, June 16, 1992

DoDD 5230.20, *Visits, Assignments, and Exchanges of Foreign Nationals*, August 12, 1998

DoDD 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure*, November 6, 1984 w/Change 1, August 18, 1995

DoD 5400.7-R/AF Sup 1, *Freedom of Information Act (FOIA) Program*, 24 June 2002

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

DoDD 8500.1, *Information Assurance*, October 24, 2002

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

DoD 8510.1-M, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual*, July 31, 2000

JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001 as amended through 14 August 2002

International Traffic in Arms Regulations (ITAR) (22 CFR Parts 120-130)

Export Administration Regulations (EAR)

AFPD 33-2, *Information Protection* (will become *Information Assurance*)

AFI 16-201, *Disclosure of Military Information to Foreign Governments and International Organizations* (to be published)

AFI 25-201, *Support Agreements Procedures*

AFI 31-401, *Information Security Program Management*

AFI 31-501, *Personnel Security Program Management*

AFI 31-601, *Industrial Security Program Management*

AFI 33-103, *Requirements Development and Processing*

AFI 33-104, *Base-Level Planning and Implementation*

AFI 33-112, *Computer Systems Management*

AFI 33-114, *Software Management*

AFI 33-115, Volume 1, *Network Management*

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

AFI 33-118, *Radio Frequency (RF) Spectrum Management*

AFI 33-137, (Draft) *Ports, Protocols, and Services (PPS) Management* (to be published)

AFI 33-201, *(FOUO) Communications Security (COMSEC)*

AFI 33-203, *Emission Security*

AFI 33-204, *Information Assurance Awareness Program*

AFI 33-205, *Information Protection Metrics and Measurements Program*

AFI 33-206, *Air Force Specialized Information Assurance Publications*

AFI 33-207, *Computer Security Assistance Program*

AFI 33-213, *DoD Public Key Infrastructure Management and Use*

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*

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

AFI 33-360, Volume 2, *Content Management Program-Information Management Tool (CMP-IMT)*

AFI 36-8002, *Telecommuting Guidelines For Air Force Reservists and Their Supervisors*

AFMAN 33-120, *Radio Frequency (RF) Spectrum Management*

AFMAN 33-214, Volume 1, *(S) Emission Security Assessments (U)*

AFMAN 33-214, Volume 2, *Emission Security Countermeasures Reviews*

AFMAN 33-223, *Identification and Authentication*

AFMAN 37-123, *Management of Records*

AFMAN 37-139 DELETED

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

AFPAM 63-1701, *Program Protection Planning*

AFSSI 5020, *Remanence Security* (will become AFMAN 33-224)

AFSSI 5021, *Time Compliance Network Order (TCNO) Management and Vulnerability and Incident Reporting*

WEB-RIMS, *Records Disposition Schedule (RDS)*

### ***Abbreviations and Acronyms***

**ADP**–Automated Data Processing

**AFCA**–Air Force Communications Agency

**AFCERT**–Air Force Computer Emergency Response Team

**AF-CIO**–Air Force Chief Information Officer

**AFI**–Air Force Instruction

**AFIWC**–Air Force Information Warfare Center

**AFMAN**–Air Force Manual

**AFMC**–Air Force Materiel Command

**AFPD**–Air Force Policy Directive

**AFSPC**–Air Force Space Command

**AFSSI**–Air Force Systems Security Instruction

**AIA**–Air Intelligence Agency

**AIS**–Automated Information System

**AP**–Access Points

**ASD/C3I**–Assistant Secretary of Defense for Command, Control, Communications and Intelligence

**ASD/NII**–Assistant Secretary of Defense for Networks and Information Integration (replaces the term ASD/C3I)

**ASIM**–Automated Security Incident Monitoring

**BIP**–Base Information Protection

**C4I**–Command, Control, Communications, Computers, and Intelligence

**C4ISP**–C4I Support Plan  
**C&A**–Certification and Accreditation  
**CAC**–Common Access Card  
**CC**–Common Criteria  
**CCB**–Configuration Control Board  
**CERT**–Computer Emergency Response Team  
**CITS**–Combat Information Transport System  
**CJCSI**–Chairman of the Joint Chiefs of Staff Instruction  
**COMPUSEC**–Computer Security  
**COMSEC**–Communications Security  
**CoN**–Certificate of Networthiness  
**CSO**–Communications and Information Systems Officer  
**CtO**–Certificate to Operate  
**DAA**–Designated Approving Authority  
**DAC**–Discretionary Access Control  
**DISA**–Defense Information Systems Agency  
**DISN**–Defense Information Systems Network  
**DITSCAP**–DoD Information Technology Security Certification and Accreditation Process  
**DoD**–Department of Defense  
**DoDD**–Department of Defense Directive  
**DRU**–Direct Reporting Unit  
**DSAWG**–DISN Security Accreditation Working Group  
**EAL**–Evaluation Assurance Level  
**EAR**–Export Administration Regulations  
**EMSEC**–Emission Security  
**FDO**–Foreign Disclosure Office  
**FIPS**–Federal Information Processing Standards  
**FOA**–Field Operating Agency  
**FOUO**–For Official Use Only  
**FTP**–File Transfer Protocol  
**GIAP**–GIG Interconnection Approval Process  
**GIG**–Global Information Grid

**GSU**–Geographically Separated Units  
**IA**–Information Assurance  
**IATO**–Interim Approval to Operate  
**IDS**–Intrusion Detection Service  
**I&A**–Identification and Authentication  
**IPO**–Information Protection Operations  
**IR**–Infrared  
**ISP**–Internet Service Provider  
**ISSM**–Information System Security Manager  
**ISSO**–Information System Security Officer  
**IT**–Information Technology  
**ITAR**–International Traffic in Arms Regulations  
**i-TRM**–Infostructure Technical Reference Model  
**JP**–Joint Publication  
**MAC**–Media Access Control  
**MAJCOM**–Major Command  
**MFD**–Multi-function Devices  
**NATO**–North Atlantic Treaty Organization  
**NCC**–Network Control Center  
**NCSC**–National Computer Security Center  
**NIAP**–National Information Assurance Partnership  
**NIPRNET**–Non-Secure Internet Protocol Router Network  
**NIST**–National Institute of Standards and Technology  
**NOSEC**–Network Operations and Security Center  
**NSA**–National Security Agency  
**OMB**–Office of Management and Budget  
**OPSEC**–Operational Security  
**PC**–Personal Computer  
**PDA**–Personal Digital Assistants  
**PED**–Personal Electronic Device  
**PKI**–Public Key Infrastructure  
**P.L.** –Public Law

**POC**–Point of Contact

**PPS**–Ports, Protocol, and Services

**RAS**–Remote Access Server

**RDS**–Records Disposition Schedule

**SABI**–Secret and Below Interoperability

**SAF**–Secretary of the Air Force

**SAF/AA**–Administrative Assistant to the Secretary of the Air Force

**SAP/SAR**–Special Access Program/Special Access Required

**SCAO**–SIPRNET Connection Approval Office

**SCD**–Systems Compliance Database

**SCI**–Sensitive Compartmented Information

**SDP**–Service Delivery Point

**SFUG**–Security Feature User’s Guide

**SIPRNET**–Secret Internet Protocol Router Network

**SSAA**–System Security Authorization Agreement

**SSWG**–System Security Working Group

**ST&E**–Security Test and Evaluation

**TCNO**–Time Compliance Network Order

**TFM**–Trusted Facility Manual

**URL**–Uniform Resource Locator

**VPN**–Virtual Private Network

**WLAN**–Wireless Local Area Network

**WM**–Workgroup Manager

### ***Terms***

**Accountability**--Process of tracing information systems activities to a responsible source.

**Accreditation**--Formal declaration by a DAA that an information system 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 (AIS)**--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 computer, a central computer system with remote terminals (e.g., mainframe), a LAN, or a Wide Area Network (WAN).

**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.

**Category**--A grouping of classified or sensitive information to which an additional restrictive label is applied to signify that personnel are granted access to the information only if they have access approval (e.g., formal access approval). Examples include proprietary, FOUO, Privacy Act, North Atlantic Treaty Organization (NATO), and compartmented 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.

**Certifier**--Individual responsible for making a technical judgment of the information systems compliance with stated security requirements and requesting approval to operate from the DAA.

**Common Criteria**--The International Common Criteria for Information Technology Security Evaluation (CC) defines general concepts and principles of information technology (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-Based Security**--Security for the information system is provided through the use of automated security features.

**Computer Network**--The constituent element of an enclave responsible for connecting computing environments by providing short-haul data transport capabilities, such as local or campus area networks, or long-haul data transport capabilities, such as operational, metropolitan or 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.

**Controlled Unclassified Information**--Information that is not classified but has some restrictions placed on it, such as export controls or exemption from the Freedom of Information Act.

**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. (**NOTE:** There are two divisions of control: management [policy, objectives, and criteria class] and internal [security requirements, mechanisms, and rules]. DoDD 8000.1, *Management of DoD Information Resources and Information Technology*, 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.

**Designated Approving Authority (DAA)**--Official with the authority to formally assume responsibility for operating an information system or network within a specified environment.

**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 mission assurance category 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 as defined in OMB A-130. 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 local area networks and the applications they host, backbone networks, and data processing centers.

**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 (Common Criteria (IS 15408)) 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 Nationals**--All individuals who are non-U.S. citizens including U.S. military personnel, DoD civilian employees and contractors.

**Formal Access Approval**--Documented approval by a data owner to allow access to a particular category of information.

**Functional System**--A specific system used, owned, operated, and maintained by a functional community

**Global Information Grid (GIG)**--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 National Security Systems (NSS) as defined in section 5142 of the Clinger-Cohen Act of 1996 (reference (f)). 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.

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

**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.

**Information** 1.--Data derived from observing phenomena and the instructions required to convert that data into meaningful information. (*NOTE:* Includes: operating system information such as system parameter settings, password files, audit data, etc.) 2. (DoD) Facts, data, or instructions in any medium or form. (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 information system (IS) and network security intrusions. The NCC conducts IPO employing hardware and software tools to enhance the security of their networks

**Information System**--1. Any telecommunications and/or computer-related equipment or interconnected system or subsystems of equipment used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice, and/or data, including software, firmware, and hardware. (*NOTE:* This includes automated information systems.) 2. (DoD) The entire infrastructure, organization, and components that collect, process, store, transmit, display, disseminate, and act on information. (JP 1-02).

**Information Systems Security Manager (ISSM)**--Principal advisor on computer security matters to DAA. (*NOTE:* DoDI 8500.2 IA Manager (IAM). The individual responsible for the information assurance program of a DoD information system or organization. While the term IAM is favored within the Department of Defense, it may be used interchangeably with the IA title Information Systems Security Manager (ISSM)).

**Information Systems Security Officer (ISSO)**--Official who manages the COMPUSEC program for an information system assigned to him or her by the ISSM; including monitoring information system activities, and ensuring that the information system is operated, maintained, and disposed of according to security policies and practices. (*NOTE:* DoDI 8500.2 IA Officer (IAO). An individual responsible to the IAM for ensuring that the appropriate operational IA posture is maintained for a DoD information system or organization. While the term IAO is favored within the Department of Defense, it may be used interchangeably with other IA titles (e.g., Information Systems Security Officer, Information Systems Security Custodian, Network Security Officer, or Terminal Area Security Officer).

**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 (IT)**--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 ser-

VICES), 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.

**IT Position Category**--Applicable to unclassified DoD information systems, 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 (reference (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 (ADP) 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 information system.

**Mission Assurance Category**--Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. DoD has three defined mission assurance categories:

**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.

**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.

**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.

**Network Security Policy**--Overall policy that is developed for the network. This policy regulates how sensitive and classified information is managed, protected, and distributed on the network. It also includes boundary protection, rules of engagement, methods of protection.

**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.

**Periods Processing**--Processing of various levels of classified and unclassified information at distinctly different times. (**NOTE:** Under periods processing, the information system [operating in dedicated security mode] is purged of all information from one processing period before transitioning to the next when there are different users with different authorizations.).

**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 information system. (Synonymous with Single Manager or Project Manager.)

**Safeguards**--Protective measures and controls prescribed to meet the security requirements of an information system. (**NOTE:** 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; media access control (MAC); discretionary access control (DAC); object reuse; or audit. Security features are a subset of information system 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 (Privacy Act), 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. (**NOTE:** Systems that are not national security systems, but contain sensitive information are subject to be protected in accordance with the requirements of the Computer Security Act of 1987 [P.L. 100-235].)

**Site Certification**--Provides assurance that the operational location has implemented the required security measures. This evaluation ensures that the integration and operation of the system is in accordance with the SSAA and a review of the local environment (threats/vulnerabilities).

**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 information system) and the threat.

**Stand-Alone System**--An information system 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 PC with removable storage media such as a floppy disk).

**Standard System**--Two or more substantively similar information systems developed for the purpose of fielding multiple copies in support of a mission, within or across MAJCOM or service lines, or DoD-wide.

**Strong Authentication**--Two of the three approved methods of authentication: something you know (password), something you have (token), or something you are (biometric).

**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.

**System Security Policy**--Set of laws, rules, and practices that regulate how sensitive and classified information is managed, protected, and distributed by an information system. (**NOTE:** It interprets regulatory [e.g., DoDD 8500.1, AFD 33-2, AFI 33-202, etc.] and operational requirements for a particular system and states how that system will satisfy those requirements. All systems or networks, regardless of their sensitivity, criticality, or life-cycle phase, will have a system security policy.)

**Tampering**--Unauthorized modification that alters the proper functioning of information system security equipment.

**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 information system by direct connections (e.g., via terminals) or indirect connections.

**Vulnerability**--1. Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited. 2. (DoD) 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. (JP 1-02) 3. (DoD) 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)

**Workgroup Manager (WM)**--A duty supporting a functional community (e.g., workcenters, flights, squadrons, or organizations) and is the first line of help customers contact to resolve problems.