

**BY ORDER OF THE SECRETARY  
OF THE AIR FORCE**

**AIR FORCE POLICY DIRECTIVE 16-14**

**28 SEPTEMBER 2010**

**Operations Support**

**INFORMATION PROTECTION**



**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

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

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

---

OPR: SAF/AAP

Certified by: SAF/AA  
(William A. Davidson)

Supersedes: AFPD14-3, 1 May 1998,  
AFPD16-2, 10 Sept 1993,  
AFPD31-4, 1 Sept 1998,  
AFPD31-5, 1 August 1995,  
AFPD31-6, 1 April 2000,  
AFPD33-2, 19 April 2007,  
AFPD63-17, 26 Nov 2001.

Pages: 12

---

This Policy Directive (PD) implements DoD Instruction 5200.01, *DoD Information Security Program and Protection of Sensitive Compartmented Information*, dated 9 October 2008 and DoD Directive 8500.01E, *Information Assurance*, dated 23 April 2007. It establishes policies and responsibilities for the oversight, management, and execution of protecting Air Force (AF) information. Regardless of the domain in which information exists, this directive provides the basis for implementing AF instructions to execute protection of that information. It consolidates selected information protection policy from AFD 10-7, *Information Operations*; AFD 33-3, *Information Management*; AFD 35-1, *Public Affairs Management*; AFD 16-6, *Arms Control Agreement*; AFD 61-2, *Management of Scientific and Technical Information*; and AFD 63-1/AFD 20-1, *Acquisition and Sustainment Life Cycle Management*. This policy applies to all military, government civilian personnel, contractors, and consultants when contract performance depends on access to AF Information Protection (IP) and security programs. This PD provides consolidated guidance for IP across the AF enterprise. This policy directs converged organizational relationships, responsibilities, and structures to effectively protect information essential to successful operations. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Form 847 from the field through functional chain of command. Supplemental instructions must have the concurrence of the OPR. Ensure that all records created as a result of processes prescribed in this publication are

maintained in accordance with AFMAN 33-363, *Management of Records*, and disposed of in accordance with the AF Records Disposition Schedule (RDS) located at <https://www.my.af.mil/gcss-af61a/afrims/afrims/>.

**1. The success of AF operations and sustainment, as well as continued technological superiority, relies on protecting its information across the enterprise.** The AF protects information across missions and functions spread among myriad organizations and operations across the globe. Due to the number of people, organizations, and missions involved, vulnerabilities in one area can have significant impact to our national security capabilities. Therefore, the AF will employ a converged, collaborative, and integrated framework to assure effective execution of IP measures. Commanders are responsible for implementation of IP measures according to policies and risk management principles.

**2. IP is the collective policies, processes, and implementation of risk management and mitigation actions instituted to prevent the compromise, loss, unauthorized access/disclosure, destruction, distortion, or non-accessibility of information, regardless of physical form or characteristics, over the life cycle of the information.** It includes actions to regulate access to sensitive information, controlled unclassified information (CUI), and classified information produced by, entrusted to, or under the control of the United States Government.

**3. IP is achieved through the implementation of the converged IP security policies from disciplines that make up IP:** information security, information assurance (IA), operations security (OPSEC), personnel security, physical security, international security (foreign disclosure, North Atlantic Treaty Organization [NATO]), industrial security, Sensitive Compartmented Information (SCI), Restricted Data (RD) and Formerly Restricted Data (FRD), Special Access Program (SAP), acquisition program protection, and Scientific and Technical Information (STINFO).

3.1. The effective training and participation of every Airman is vital to success. Therefore, all personnel must be trained according to their access and responsibilities and be tasked to protect information consistent with threats, mission, and national security policy.

3.2. Regardless of format, information will be monitored, defended, and protected commensurate with the shared risk and potential harm that could result from disclosure, loss, misuse, alteration, or destruction of the information or system.

3.3. Each echelon of command will assess IP effectiveness and trends within its purview. This measurement will encompass, but is not limited to, federal and DoD IA reporting requirements.

3.4. IP will be implemented in all acquisitions at levels appropriate to the system characteristics and requirements throughout the acquisition life cycle. Acquisitions shall comply with DoDI 8500.2, *IA Implementation*, and DoDI 8580.1, *Information Assurance*, in the Defense Acquisition System. IP will be implemented in space systems according to DoDD 8581.1E, *IA Policy for Space Systems Used by the Department of Defense*.

3.5. Intelligence information will be controlled and protected to preserve the integrity of the intelligence collection system to include implementing enhanced SCI safeguards.

#### **4. Roles and responsibilities.**

#### 4.1. The Secretary of the AF (SecAF):

4.1.1. Provides senior-level policy direction and guidance relating to the protection of information; provides a unified perspective on IP policy, issues, methodologies, and structures.

4.1.2. Charters the AF Security Policy and Oversight Board (AFSPOB) to provide oversight, establish objectives, and assess IP security progress at least semiannually. The AFSPOB will:

4.1.2.1. Ensure an enterprise-wide and converged organization perspective to security policy development, oversight, implementation, and training. The AFSPOB provides a unified AF perspective on security policy issues across the Service as well as to DoD, executive agencies, and other external organizations.

4.1.2.2. Be composed of senior leaders representing Headquarters AF (HAF) organizations with management responsibility for IP and security functions.

4.1.2.3. Review policy for SecAF approval, provide oversight, and ensure that functional training issues are addressed and sufficient resources are available to manage and sustain requirements across the AF enterprise.

4.1.2.4. Review and report metrics on security program performance across the enterprise, and provide an annual report on the state of AF IP programs.

4.1.3. Designates Original Classification Authorities (OCAs) at the Top Secret, Secret, and Confidential levels.

4.1.4. Serves as the disclosure authority for National Disclosure Policy as it pertains to disclosure or denial of military information originated within the AF to foreign nationals.

#### 4.2. The Administrative Assistant to the Secretary of the AF (SAF/AA):

4.2.1. Represents SecAF as the AF Senior Security Official, providing:

4.2.1.1. Oversight and broad direction collectively with other senior staff members on plans, policies, and programs related to AF-wide IP/assurance and personnel, industrial, physical, network/computer, and information security.

4.2.1.2. Policy and oversight of all AF SAPs.

4.2.1.3. RD/FRD Management Official to provide oversight for accountability, training, and provision of accurate guidance for handling, safeguarding, protecting, or releasing nuclear-related information pursuant to the Atomic Energy Act of 1954; 10 CFR Part 1045, *Nuclear Classification and Declassification*; and DoD Directive 5210.2, *Access to and Dissemination of Restricted Data*.

4.2.1.4. Is the Designated Approval Authority (DAA) for SAPs.

4.2.2. Chairs the AFSPOB and maintains a Secretariat staff within the Directorate of Information Protection (SAF/AAP) to provide administrative and operational support to the Board.

- 4.2.3. Designates the Director, Information Protection (SAF/AAP), to chair the AF Security Advisory Group (AFSAG). The AFSAG is responsible for articulating policy, formulating associated processes, and overseeing AF-wide implementation.
- 4.2.4. Delegates OCA at the Secret and Confidential level.
- 4.2.5. Designates the Director, Security, Counterintelligence and Special Program Oversight (SAF/AAZ), as the responsible individual for providing general oversight of all SAPs for which the AF has responsibility. This position is also the Director for the AF Special Access Program Central Office (SAPCO). Establishes SAP security policies and procedures for all SAPs for which the AF has responsibility and ensures compliance within the National Security construct through guidelines, inspections, regulations, and other measures.
- 4.2.6. Designates the Director, AF Central Adjudication Facility (AFCAF), as the responsible individual to ensure quality and timely security clearance eligibility determinations, trustworthiness, and SAP determinations for all active duty, Air National Guard, Reserve, and civilian personnel and grants SCI eligibility to contractor personnel for the United States AF.
- 4.2.7. Delegates responsibilities for functional area guidance subordinate to this policy directive.
- 4.3. The Assistant Secretary of the AF for Acquisition (SAF/AQ) is responsible for ensuring IP is incorporated into policy, training, and resource advocacy as applicable to assigned acquisition programs.
- 4.4. The Deputy Undersecretary of the AF for International Affairs (SAF/IA):
- 4.4.1. On behalf of the SecAF, serves as the Principal Disclosure Authority for the AF. Develops disclosure policy for SecAF approval, delegates disclosure authority, and represents the AF on the National Disclosure Policy Committee (NDPC).
- 4.4.2. Develops and manages the AF foreign disclosure program via the Foreign Disclosure and Technology Transfer Division.
- 4.5. The Director of Public Affairs (SAF/PA) is:
- 4.5.1. Responsible for coordinating the review of information that is proposed for public release and for ensuring that it does not contain sensitive, unclassified controlled, or classified material and does not conflict with established AF, DoD, or US Government policy.
- 4.5.2. Responsible for overseeing the public clearance process by the Public Affairs Officer at the lowest level where competent authority exists to judge the security and policy aspects of the information being submitted for review.
- 4.6. The Chief of Warfighter Integration and Chief Information Officer (SAF/A6 CIO):
- 4.6.1. Develops, sustains, and maintains overall responsibility for the AF IA program.
- 4.6.2. On behalf of SECAF, implements all IA related responsibilities designated for the Head of DoD Components as outlined in DoD 8000 series Directives and Instructions.

- 4.6.3. Develops, approves, and enforces IA policies in accordance with statutory requirements outlined in the Federal Information Security Management Act and serves as the DoD focal point for all IA-related matters.
- 4.6.4. On behalf of the SecAF, appoints Designated Accrediting Authorities (i.e., Authorizing Officials) and the Senior Risk Executive for the AF enterprise network.
- 4.6.5. Coordinates with Joint and Defense-wide program offices to ensure interoperability of IA solutions across the DoD enterprise.
- 4.6.6. Defines IA performance measures to identify enterprise-wide IA trends, to include IA-related vulnerabilities, Plan of Action and Milestones (POA&M) to mitigate the vulnerabilities, and an updated status of mitigation efforts.
- 4.6.7. Appoints the Senior Information Assurance Officer as mandated by FISMA and submits the annual of all IA-related metrics required under FISMA to DoD Chief Information Officer (CIO).
- 4.6.8. Approves acquisition IA strategies for submission to the DoD CIO.
- 4.6.9. Develops Information Management (IM) policy for SecAF approval, providing guidance and procedures for Records Management (RM), Freedom of Information Act (FOIA), Privacy Act (PA), Federal Register, Military Postal Service, Official Mail/Distribution, and Information Collections and Reports Control.
- 4.6.10. Ensures IA awareness training, education, and professionalization are provided to all AF personnel commensurate with their respective responsibilities for developing, using, operating, administering, maintaining, and retiring AF information systems.
- 4.6.11. Complies with DoD established accreditation and connection approval processes required for all DoD information systems.
- 4.7. The Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance (AF/A2):
  - 4.7.1. Represents AF as the Head of the AF Element of the Intelligence Community responsible for intelligence information security for the AF and is the approval authority for issues involving the release of intelligence information.
  - 4.7.2. Maintains effective control of the dissemination of intelligence information among US intelligence community components, US forces outside the intelligence community requiring the information, foreign nationals, foreign governments, and contractors.
  - 4.7.3. Appoints the AF Cognizant Security Authority (CSA) for SCI. The CSA is the designated responsible official for SCI security program management.
  - 4.7.4. Ensures AF Service Cryptologic Elements comply with National Security Agency directives. Conflicts will be resolved by the designated CSA.
  - 4.7.5. Establishes intelligence security control and release programs and oversees Major Command (MAJCOM), Field Operating Agency (FOA), and Direct Reporting Unit (DRU) intelligence security programs.
  - 4.7.6. Represents the AF in national and DoD intelligence security forums.

- 4.7.7. Integrates IA capabilities into the protection of SCI and ensures SCI systems' accreditation.
  - 4.7.8. Establishes objectives and requirements for the electronic exchange and dissemination of security and intelligence information through automated security management systems.
  - 4.7.9. Provides SAF/AA, SAF/XC, SAF/AQ, SAF/US, AFNETOPS, and other appropriate organizations with threat information concerning current and emerging threats to AF security.
  - 4.7.10. Provides threat information to support risk management and awareness.
- 4.8. The Deputy, Chief of Staff for Operations, Plans and Requirements (AF/A3/5):
- 4.8.1. Serves as the OPR for AF Information Operations (IO) and Cyberspace Operations doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) considerations.
  - 4.8.2. Serves as the OPR for each of the IO and Cyberspace Operations capabilities (inclusive of OPSEC, but excluding Public Affairs and Counterintelligence) and for integrating IO capabilities.
  - 4.8.3. Ensures the incorporation of standardized IO and Cyberspace Operations requirements into AF acquisition activities.
  - 4.8.4. Coordinates overall IO and Cyberspace Operations policy development, doctrine, strategy, and investment priorities with other HAF offices having IO responsibilities. AF/A3/5 coordinates on all IO-related matters to include promulgation of policy and guidance, requirements derivation, and programmatic issues.
  - 4.8.5. In conjunction with SAF/A6 CIO, identifies relevant performance measures and metrics for IA's Integrated Control Enabler capabilities for information operations; and advocates for improved capabilities for those enablers.
  - 4.8.6. Develops AF critical infrastructure strategy and policy for SecAF approval. This function also prepares objectives; implements plans and programs; and advocates plans, operations, and funding to departmental and governmental agencies.
- 4.9. The Deputy, Chief of Staff for Logistics, Installations and Mission Support (AF/A4/7):
- 4.9.1. Establishes the AF framework for formulating and implementing SecAF-approved Integrated Defense (ID) policy and capabilities to mitigate vulnerabilities, reduce risks, and neutralize/defeat ground threats to AF operations.
  - 4.9.2. Provides physical security to facilities and programs protecting CUI and NSI.
- 4.10. The Assistant Chief of Staff Strategic Deterrence & Nuclear Integration (AF/A10):
- 4.10.1. Standardizes nuclear-related IP actions that ensure safe, secure, and reliable nuclear operations.
  - 4.10.2. Is the single HAF staff authority to ensure uniformity of the nuclear enterprise policy, guidance, requirements, and advocacy. Provides staff oversight to ensure synchronization and integration of related issues across the nuclear enterprise.

4.11. The Inspector General (SAF/IG) assesses the security readiness, discipline, efficiency, and economy of the AF and the Air National Guard and reports findings to the AFSPOB, SecAF, and the AF Chief of Staff.

4.12. The Commander of the AF Office of Special Investigations (AFOSI) to the extent authorized by statute, Executive Order, and regulation:

4.12.1. Performs as a federal law enforcement agency with responsibility for conducting independent criminal investigations, counterintelligence activities, and specialized investigative and force protection support for the AF.

4.12.2. Provides counterintelligence functional services such as conducting Human Intelligence Vulnerability Assessments (HVAs), Antiterrorism Surveys, Counterintelligence Force Support Operations, and Threat Assessments.

4.12.3. Is the sole AF organization authorized to investigate intrusions into and sabotage of AF- owned/operated DoD computer systems.

4.13. Commanders and Directors of MAJCOM, DRU, FOA and installations:

4.13.1. Are responsible for the defense of the installation's infrastructure, personnel, information, activities, and resources; will conduct risk estimates, implement mitigation, and accept risk for power projection and mission support assets consistent with higher echelon intent; and will establish IP programs and identify requirements to comply with this policy. The MAJCOM, DRU, and FOA Vice Commanders/Deputy Directors are designated the Senior Security Officials for their respective organizations.

4.13.2. Appoint a Director (at MAJCOM) or Chief (at installations) of Information Protection to manage the Information Protection Office (IPO) and staff. They serve as the Director, Information Protection, or a Chief, dependent on organizational echelon, to lead their IP office and staff. The Director or Chief of IP serves as the single focal point to converge multifunctional security issues. The IP office provides the secretariat function for the respective echelon's Security Advisory Group (SAG). Appointing officials will ensure security managers and other personnel in IP-related positions receive required training.

4.13.3. Charter a SAG comprised of organizations of subject matter experts within their organizational echelon with responsibility for coordinating and implementing IP-related functions.

4.13.4. Identify positions requiring access to classified information, continuously evaluate those persons with access, and promptly report adverse information on cleared personnel.

4.13.5. Ensure appropriate personnel security investigations are promptly requested, completed, and adjudicated before individuals are given access to classified information or assigned to sensitive duties.

4.13.6. Establish an industrial security program and provide oversight for subordinate activities. Installation Commanders will ensure program implementation and program oversight.

4.13.7. Designate command foreign disclosure officers (FDOs) and ensure the command disclosure program is effective and under delegated disclosure authority from SAF/IA.

4.13.8. Ensure, as host MAJCOM for an installation, that SCI communications and security management are provided as necessary to support any AF unit mission on that installation.

4.13.8.1. Commanders/Head Intelligence Officers (HIOs) will ensure facilities where intelligence information is used meet security requirements and personnel are trained to protect the information.

4.13.8.2. Commanders/HIOs may enter into agreements (Memorandums of Agreement) with other United States security organizations to provide or receive security services. The sharing or consolidation of security resources and skills required to meet the needs of the participant's individual governing directives is encouraged.

4.13.8.3. The host command may contract with a tenant organization to provide SCI communications and SCI security management oversight at an AF installation for the host command. To conserve resources and remove duplicity of functions, if requested by installation tenant security officials, the installation Special Security Office (SSO) will provide certain core functions and responsibilities that are considered operational standards for all SSOs. This isn't meant to cross command lines of authority nor consolidate multiple SSOs belonging to different Commands on a base/installation.

4.13.9. Commanders and program office managers must identify programs requiring SAP controls and, once these programs are approved, must comply with SAP policy.

## **5. Commanders/Directors:**

5.1. Establish, sustain, and resource IP education, training, awareness, and professionalization programs commensurate with the command and functional responsibilities.

5.2. Commanders are responsible for managing risk to information under their responsibility or control, including information transitioning through their control. Commanders will protect information and the systems that store, transmit, and/or receive information and ensure incidents and compromises are reported and mitigated.

5.3. Identify NSI and CUI and sensitive resources unique to their programs or projects that must be protected. These activities will incorporate appropriate security classification guidance, if applicable, and handling, processing, marking, and safeguarding requirements into all solicitations.

5.4. Integrate on-base contractor visitor groups into the host installation's IP environment unless mission, operational requirements, autonomous nature, or other factors necessitate a separate security program under the *National Industrial Security Program Operating Manual* (NISPOM).

5.5. Implement security policies and procedures consistent with the standards of the NISPOM, Information Security Program, and Federal Acquisition Regulations (FAR) where industrial accounts are established.

5.6. Ensure contracts requiring access to sensitive and classified information for which contractual security specifications identify safeguards and/or protection requirements are coordinated and thoroughly reviewed by the appropriate security activity and functional area or OPR prior to issuing the solicitation.

5.7. Ensure activities which classify and/or maintain classified holdings implement an automatic declassification program. These activities should identify and review classified information that is more than 25 years old. Classified information determined to have permanent historical value under Title 44, United States Code, should be scheduled for transfer to the legal custody (accession) of the National Archives in accordance with AFI 33-364, *Records Disposition - Procedures and Responsibilities*. Coordinate scheduled transfers with the AF Declassification Office.

5.8. Control intelligence information in accordance with governing directives and report intelligence information security violations to the respective Wing A2 organization.

5.9. Conduct security awareness training with emphasis on reducing or preventing violations.

5.10. Continuously evaluate organizational efficiency and effectiveness through a converged multifunctional assessment process.

5.11. Ensure coordinated and collaborative execution of AF IP policies and processes on joint bases and for expeditionary operations.

5.12. Ensure effective implementation of IA policies and procedures on AF-owned or controlled information systems. IP processes and IA requirements shall be included in AF system design, acquisition, installation, operation, upgrade, disposition, or replacement actions.

Michael B. Donley  
Secretary of the Air Force

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

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

AFPD 71-1, *Criminal Investigations and Counterintelligence*, January 6, 2010

AFPD 33-3, *Information Management*, March 28, 2006

DCID 1/19, *Security Policy for Sensitive Compartmented Information*, March 1, 1995

DoD 5200.1-R, *DoD Information Security Program Regulation*, January 1997

DoDD 8500.01E, *Information Assurance*, April 2007

DoDI 8500.2, *Information Assurance Implementation*, February 2003

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

DODD 8000.01, *Management of the Department of Defense Information Enterprise*, February 10, 2009

DoDI 8510.01, *DoD IA Certification and Accreditation Process (DIACAP)*, November 28, 2007

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

DODI 5200.01, *DoD Information Security Program and Protection of Sensitive Compartmented Information*, October 9, 2008

10 U.S.C. § 119, *Special Access Programs: Congressional Oversight*

44 U.S.C. Subsection, 3542, *Federal Information Security Management Act*

Executive Order 13526, *Classified National Security Information*, December 29, 2009

Federal Register Part VI, Office of Management and Budget, *Title 32, National Defense CFR Part 2001 and 2004, Information Security Oversight Office; Classified National Security Information; Final Rule*, September 23, 2003

AFPD 16-6, *Arms Control Agreements*, February 25, 2004

AFPD 35-1, *Public Affairs Management*, September 17, 1999

TCG-WPMU-2, *Joint DOE/DoD Topical Classification Guide for Weapon Production and Military Use (U)*, September 9, 2004

***Abbreviations and Acronyms***

**AFI**— Air Force Instruction

**AFMAN**— Air Force Manual

**AFPD**— Air Force Policy Directive

**AFSPOB**— Air Force Security Policy Oversight Board

**CFR**— Code of Federal Regulations

**CISO**— Chief Information Security Officer  
**CSA**— Cognizant Security Authority  
**CUI**— Controlled Unclassified Information  
**DAA**— Designated Accreditation Authorities  
**DCID**— Director of Central Intelligence Directive  
**DoD**— Department of Defense  
**DOE**— Department of Energy  
**DRU**— Direct Reporting Unit  
**EO**— Executive Order  
**FDO**— Foreign Disclosure Officer  
**FISMA**— Federal Information Security Management Act  
**FOA**— Field Operating Agency  
**FOIA**— Freedom of Information Act  
**HAF**— Headquarters Air Force  
**HIO**— Head Intelligence Officer  
**HVA**— Human Intelligence Vulnerability Assessment  
**IA**— Information Assurance  
**IP**— Information Protection  
**ID**— Integrated Defense  
**IO**— Information Operations  
**ISOO**— Information Security Oversight Office  
**ISPM**— Information Security Program Manager  
**IM**— Information Management  
**MAJCOM**— Major Command  
**NARA**— National Archives and Records Administration  
**NDPC**— National Disclosure Policy Committee  
**NSI**— National Security Information  
**OPR**— Office of Primary Responsibility  
**PA**— Privacy Act  
**RM**— Resource Management  
**SAG**— Security Advisory Group  
**SAP**— Special Access Program

**SCI**— Sensitive Compartmented Information

**SECAF**— Secretary of the Air Force

**SIAO**— Senior Information Assurance Official

**SPOC**— Special Program Oversight Committee

**UCMJ**— Uniform Code of Military Justice