BY ORDER OF THE SECRETARY
OF THE AIR FORCE

AIR FORCE INSTRUCTION 16-1401

29 JULY 2019

Operations Support

INFORMATION PROTECTION

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication

OPR: SAF/AAZ

Certified by: SAF/AA
(Mr. Anthony P. Reardon)
Pages: 12

This publication implements Air Force Policy Directive (AFPD) 16-14, *Air Force Security Enterprise Governance*. It provides guidance and procedures for the oversight, management and execution of the Information Protection programs throughout the Air Force (AF). It applies to individuals at all levels including the Air Force Reserve and Air National Guard, except where noted otherwise. This publication may be supplemented at any level, but all supplements must be routed to the office of primary responsibility listed above for coordination prior to certification and approval. Refer recommended changes and questions about this publication to the office of primary responsibility listed above using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate chain of command. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See Air Force Instruction (AFI) 33-360, *Publications and Forms Management* for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the requestor's commander for non-tiered compliance items. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule located in the Air Force Records Information Management System.

Chapter 1

INFORMATION PROTECTION PROGRAM OVERVIEW

1.1. Information Protection. Information Protection is a subset of the Air Force Security Enterprise. Information Protection consists of a set of three core security disciplines (Personnel, Industrial, and Information Security) used to:

1.1.1. Determine military, civilian, and contractor personnel's eligibility to access classified information or occupy a sensitive position. (Personnel Security).

1.1.2. Ensure the protection of classified information that may be released or has been released to current, prospective, or former contractors, licensees, or grantees of United States agencies. (Industrial Security).

1.1.3. Protect classified information that, if subject to unauthorized disclosure, could reasonably be expected to cause damage to national security. Protect controlled unclassified information (CUI) which may be withheld from release to the public. (Information Security).

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Administrative Assistant to the Secretary of the Air Force (SAF/AA). The combination of information security responsibilities with personnel and industrial security responsibilities assigned by Headquarters Air Force (HAF) Mission Directive 1-6, *Administrative Assistant to the Secretary of the Air Force,* makes SAF/AA responsible for the Air Force Information Protection Programs.

2.1.1. Serves as the Senior Agency Official.

2.1.2. Serves as the Air Force Security Program Executive.

2.2. The Director of Security, Special Program Oversight and Information Protection (SAF/AAZ) serves as the pertinent oversight authority (defined in AFI 90-201, *The Air Force Inspection System)* and functional for Information Protection. SAF/AAZ directs oversight inspections and self-assessments. **SAF/AAZ shall:**

2.2.1. Serve as the principal advisor to the Administrative Assistant to the Secretary of the Air Force (SAF/AA).

2.2.2. Develop policy and guidance for the Air Force Information Protection Programs.

2.2.3. Define Information Protection inspection and assessment criteria and evaluate security compliance trends for potential changes in policy, training, and assessment and inspection.

2.3. Assistant Secretary of the Air Force for Acquisition, Technology & Logistics (SAF/AQ):

2.3.1. Develops policy and procedures for implementing security and protection requirements in solicitations and contracts in support of the National Industrial Security Program.

2.3.2. Ensures integration and collaboration with engineering, security, logistics, and intelligence activities to develop policy and processes to manage malicious or subversive exploitation of the supply chain.

2.3.3. Ensures engineering processes and technical analysis incorporate methodologies and techniques to identify information, components and technologies vital to warfighting capability, and integration of engineering and security measures to protect the information, components, and technologies from known security threats and attacks.

2.3.4. Establishes integrated life cycle acquisition implementing policy and guidance for protection of Air Force systems, subsystems, end-items, and services.

2.4. The International Affairs Directorate of Policy, Programming, and Strategy Directorate of the Deputy Under Secretary of the Air Force (SAF/IAP):

2.4.1. Directs, administer, and oversee the Air Force Foreign Disclosure Program pertaining to foreign government information, the disclosure of classified information and CUI to foreign governments and international organizations, and security arrangements for international programs.

2.4.2. Collaborates with SAF/AAZ to develop and coordinate information protection policy as it pertains to security cooperation.

2.5. Directorate of Force Development (AF/A1D): provides guidance for integrating and vetting new/emerging institutional education and training requirements or learning outcomes into accessions, professional military education, professional continuing education and ancillary training to include security education and training.

2.6. Directorate of Civilian Force Management Directorate (AF/A1C):

2.6.1. Oversees implementation and sustainment of civilian personnel policies (recruitment, classification, placement, workforce shaping and planning, compensation, performance management, benefits, entitlements, work/life, employee relations, labor relations) to include all occupational series 0080 Security Specialists.

2.6.2. Ensures civilian performance rating/appraisal systems include the designation and management of classified information as a critical element or item to be evaluated.

2.7. Directorate of Manpower, Organization & Resources (AF/A1M):

2.7.1. Is responsible for defining AF manpower requirements and managing corporate AF Manpower and Personnel programming and resource distribution for the Total Force; and ensure corporate AF manpower requirements link mission capabilities to programmed resources.

2.7.2. Notifies SAF/AA of changes to manpower and career field requirements that will impact the Personnel Security Investigations budget on a semi-annual basis.

2.8. Directorate of Force Management Policy (AF/A1P): ensures military performance rating/appraisal systems include the designation and management of classified information as a critical element or item to be evaluated.

2.9. Directorate of ISR Special Programs (AF/A2Z): provides expertise and guidance as the lead for sensitive compartmented information protection to include all actions regarding the security, use, and dissemination thereof.

2.10. Directorate of Security Forces (AF/A4S): develops and provides integrated defense doctrine, policies and plans to protect and defend air, space and cyberspace assets, missions and personnel.

2.11. Deputy Chief Information Officer (SAF/CN): provides oversight and policy guidance to enable mission assurance through effective cybersecurity risk management specifically as it relates to CUI protection and Air Force Damage Assessment Management Office (SAF/CNZ).

2.12. Capabilities Division (AF/A10C): serves as lead for issues impacting the Air Force Nuclear Enterprise to include the classification and declassification of nuclear information (restricted data and formerly restricted data) in support of the Air Force Restricted Data Management Official (SAF/AA).

2.13. The Commander, Headquarters United States Air Forces in Europe - Air Force Africa (USAFE-AFAFRICA) shall: serve as the Air Force Executive Agent for the North Atlantic Treaty Organization (NATO) Safeguarding Program. The USAFE-AFAFRICA Director, Information Protection represents the Air Force at NATO meetings and interagency forums, and forwards requests to establish and disestablish AF sub-registries to the Central United States Registry. **(T-1)**

2.14. The Commander, Air Force Materiel Command (AFMC) shall: serve as the AF security cooperation program management lead for security and information protection. Ensures recipient foreign governments have both the capability and intent to protect releasable classified information and materials, and CUI to the equivalent U.S. government standards. **(T-1)**

2.15. The Commander, Air Combat Command (ACC) shall: serve as the Air Force sanitization lead for data spills/classified message incident reporting via the Twenty-Fourth Air Force (AFCYBER). **(T-1)**

2.16. Major Command (MAJCOM)/Direct Reporting Unit (DRU)/Field Operating Agency (FOA) Commanders/Directors:

2.16.1. Shall appoint a Command Security Program Executive. **(T-1)**

2.16.2. Collaborate with the Command Security Program Executive to communicate and coordinate on security issues relative to their command and implement a standardized command security structure to support an enterprise framework.

2.16.3. Integrate the various security functions to ensure consistent compliance and risk management through standardized guidelines, inspections, regulations and other measures.

2.17. MAJCOM/DRU/FOA Director, Information Protection. The senior civilian security specialist who:

2.17.1. Advises the SPE on security enterprise and information protection issues within the command.

2.17.2. Is responsible for integrating information protection into MAJCOM/DRU/FOA operations.

2.17.3. Provides oversight and direction to security specialists assigned to the MAJCOM/DRU/FOA Information Protection Directorate.

2.17.4. Provides program management, oversight, risk management, policy and guidance to subordinate units within the command.

2.17.5. Ensures damage assessments are completed in accordance with DoD Manual (DoDM) 5200.01 Volume 3, *DoD Information Security Program*: *Protection of Classified Information*, and AFI 16-1404, *Air Force Information Security Program*, when required.

2.18. Wing Commanders/Directors or Air Force Installation Commanders (when more than one Wing resides on an installation) shall:

2.18.1. Provide oversight of information protection by ensuring security controls, safeguards, and countermeasures are established through application of risk management principles, as appropriate, for their wing(s) and tenant organizations residing on their installations when documented in support agreements. **(T-2)** This responsibility may be delegated to the Deputy Commander. Tenant organization commanders, with a dedicated activity security manager, may opt to maintain independent oversight of their Information Protection programs.

2.18.2. Appoint an individual(s) as an activity security manager, assistant security manager(s) and/or security assistant(s) when required based on the level and complexity of the organization’s security program. **(T-1)**

2.18.3. Ensure military and civilian personnel are properly cleared for access to classified information, integrate contractors into their existing security programs, and protect classified information and CUI under their authority to enable information protection. **(T-0)**

2.19. Chief, Information Protection shall:

2.19.1. Execute information protection on behalf of the wing commander or installation commander, whichever applies, and provide oversight and direction to group and squadron commanders, directors, activity security managers, assistant security managers, security assistants, and the security specialists assigned to the Wing Information Protection Office. **(T-1)**

2.19.2. Serve as the activity security manager and is responsible for the overall management, functioning and effectiveness of the information protection program on behalf of the wing commander or deputy commander, as designated. **(T-1)** Activity security managers perform the duties described in Enclosure 2 and Section 9 of DoDM 5200.01, Volume 1, *DoD Information Security Program*: *Overview, Classification, and Declassification,* as determined by the commander/director. **(T-0)** The commander/director may elect to assign specific duties to other designated personnel as long as program management requirements described in DoDM 5200.01, Volume 1, Enclosure 2, and Section 9 are met. Within the Information Protection Office, the activity security manager will also perform duties described in DoDM 5200.02_AFMAN 16-1405, *Air Force Personnel Security Program,* and AFI 16-1406, *Air Force Industrial Security Program.* **(T-1)**

2.19.3. Serve as the commander’s principal advisor on the implementation of the Air Force’s Personnel, Industrial, and Information Security programs. **(T-1)** These programs are used to define risk associated with the protection of collateral classified national security, controlled unclassified, and other sensitive information as identified in AFI 38-101, *Air Force Organization*.

2.19.4. Establish, develop, coordinate and implement AF security enterprise activities, policies and procedures for the oversight, execution, management, risk management, and administration of their respective core security disciplines. **(T-1)**

2.19.5. Conduct an annual self-inspection on major areas identified in AFI 16-1404, DoDM 5200.02_AFMAN 16-1405 and AFI 16-1406, to evaluate the effectiveness and efficiency of the Information Protection Program areas. **(T-1)** These inspections will be on all organizations within their Wing and any other organizations being supported through support agreements, Memorandums of Understanding, Memorandums of Agreement, or supplements. **(T-1)**

Chapter 3

ENTERPRISE PROTECTION RISK MANAGEMENT TOOL

3.1. Enterprise Protection Risk Management Tool. The Enterprise Protection Risk Management tool is a web-based, cross-disciplinary decision support tool for security compliance and risk assessments. It facilitates and standardizes risk assessment processes and promotes early implementation of cost-effective countermeasures. The Enterprise Protection Risk Management tool has an Information Protection module that assesses all major areas of the Information, Personnel, and Industrial Security Programs.

3.2. Information Protection Offices : Shall use the Enterprise Protection Risk Management (EPRM) tool, or successor system, as the system of record to support commanders in making informed risk management decisions. **(T-1)**

3.3. Information Protection Offices : Shall use EPRM to complete the Information Security Oversight Office annual inspection report and to document inspections for compliance. **(T-1)** EPRM may also be used to document unit self-assessments in accordance with AFI 90-201.

Chapter 4

SECURITY, EDUCATION, TRAINING AND AWARENESS

4.1. All commanders and directors will: Ensure their personnel receive security education, training, and awareness. The minimum training requirements shall be completed as outlined in AFI 16-1404 and AFI 36-2645, *Security Professional Certification and Development.* **(T-0)**

4.2. Information Protection Offices: May develop additional curricula and training for assistant security managers and individuals appointed as security assistants, commensurate with their duties and responsibilities.

ANTHONY P. REARDON
Administrative Assistant

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

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

DoDM 5200.01, Volume 1, *DoD Information Security Program*: *Overview, Classification, and Declassification*, 24 February 2012

DoDM 5200.01, Volume 3, *DoD Information Security Program*: *Protection of Classified Information*, 24 February 2012, Incorporating Change 2, 19 March 2013

DoDM 5200.02, *Procedures For The DoD Personnel Security Program (PSP)*, 3 April 2017

HAF Mission Directive 1-6, *Administrative Assistant to the Secretary of the Air Force*, 22 December 2014

AFPD 16-14, *Air Force Security Enterprise*, 24 July 2014

AFI 16-1404, *Air Force Information Security Program*, 29 May 2015

AFI 16-1406, *Air Force Industrial Security Program*, 25 August 2015

AFI 33-360, *Publications and Forms Management*, 1 December 2015

AFI 36-2645, *Security Professional Certification and Development*, 2 February 2017

AFI 38-101, *Air Force Organization*, 31 January 2017

AFI 90-201, *The Air Force Inspection System*, 20 November 2018

DoDM 5200.02_AFMAN 16-1405, *Air Force Personnel Security Program*, 1 August 2018

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

Prescribed Forms

None

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AF—Air Force

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

CUI—Controlled Unclassified Information

DoD—Department of Defense

DoDI—Department of Defense Instruction

DoDM—Department of Defense Manual

DRU—Direct Reporting Unit

EPRM—Enterprise Protection Risk Management

FOA—Field Operating Agency

HAF—Headquarters Air Force

MAJCOM—Major Command

NATO—North Atlantic Treaty Organization

U.S.—United States

USAFE—United States Air Forces in Europe

Terms

Activity Head—The head, either military or civilian, of organizations, commands, and staff elements subordinate to MAJCOMs, with jurisdiction over and responsibility for the execution of the organization's mission and functions, including its information security program. The official may variously carry the title of commander, commanding officer, or director, or other equivalent title. The Activity Head will determine whether he or she requires an Activity Security Manager, Assistant Security Manager and/or Security Assistant.

Activity Security Manager (Information Protection Office)—Manages and implements the activity's information security program and ensures its visibility and effectiveness on behalf of the activity head, who retains the responsibility for overall management and functioning of the program. The activity security managers are United States (U.S.) Government civilian or military members and must have sufficient delegated authority to ensure that personnel adhere to program requirements, and their position within the organizational hierarchy must ensure their credibility and enable them to raise security issues directly to their respective activity head.

Air Force Security Enterprise—The organizations, infrastructure, and measures (to include policies, processes, procedures, and products) in place to safeguard Air Force personnel, information, operations, resources, technologies, facilities, and assets against harm, loss, or hostile acts and influences. The Air Force Security Enterprise is a blend of security, protection, and resilience programs which include: personnel, physical, industrial, information, and operations security as well as critical asset risk management; chemical, biological, radiological and nuclear response and passive defense; energy and critical infrastructure security; special access program security; critical program information protection; security planning and policy for acquisition life cycle management; antiterrorism; insider threat; and security training. Air Force Security Enterprise aligns with counterintelligence, intelligence, information operations, foreign disclosure, security cooperation, technology transfer, export control, cyber security (including defense industrial base initiatives), nuclear physical security, force protection, and mission assurance.

Assistant Security Manager—In large activities and where circumstances warrant, activities may designate U.S. Government civilian or military members as assistant security manager(s) to assist the activity security manager with program implementation, maintenance, and local oversight.

Industrial Security—Those policies, practices and procedures that ensure the safeguarding of classified information in the hands of U.S. industrial organizations, education institutions, and all organizations and facilities used by prime and subcontractors, collectively referred to as "industry."

Information Security—The system of policies, procedures, and requirements established in accordance with Executive Order 13526 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security. The term also applies to policies, procedures and requirements established to protect CUI, which may be withheld from release to the public in accordance with statute, regulation, or policy. Reference DoDM 5200.01 Volume 3.

Oversight—Authority to monitor, review, analyze, and advise on an organization's management, operations, performance, and processes through policy, guidelines, instructions, regulations or other structures to maintain compliance and effectiveness within the National Security construct.

Personnel Security—Those policies, practices and procedures which ensure that acceptance and retention of personnel in the Armed Forces, acceptance and retention of civilian employees in the Department of Defense, and the granting of members of the Armed Forces, DoD civilian employees, DoD contractors, and other affiliated persons access to classified and sensitive information are clearly consistent with the interests of national security.

Security—DoD Dictionary defines as "Measures taken by a military unit, activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness. A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences." AF Security Enterprise defines as proactive measures adopted to safeguard personnel, information, operations, resources, technologies, facilities, and foreign relations against harm, loss, or hostile acts and influences.

Security Specialists—Civilians in the Office of Personnel Management occupational series 0080, Security Administration, or military personnel assigned security as an additional duty. They are responsible for implementing Information Protection core security disciplines.

Security Assistant (formerly unit security manager)—U.S. Government civilian, military, or contractor employees who perform administrative security functions under the direction of their Commander/Director or Activity Security Manager without regard for job series, title, or rank, rate or grade provided they have the clearance required for the access needed to perform their assigned duties and tasks.

Security Program Executive—The designated individual with responsibility for and authority to accomplish security program objectives for development, production, and sustainment to meet operational needs. The Security Program Executive shall be accountable for credible cost, schedule, and performance reporting to the Defense Security Executive. At the HAF, this is SAF/AA and at the MAJCOM/DRU/FOA, this is usually the Deputy Commander

Senior Agency Official—An official appointed by the Head of a DoD Component to direct and administer the Component's Information Security program.

Sensitive Compartmented Information—Classified national intelligence information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established by the Director of National Intelligence.