BY ORDER OF THE SECRETARY OF THE AIR FORCE

DEPARTMENT OF THE AIR FORCE INSTRUCTION 16-1401

3 FEBRUARY 2023

Operations Support

INFORMATION PROTECTION PROGRAM

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**

RELEASABILITY: There are no release restrictions on this publication

---

OPR: SAF/AAZ

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

Supersedes: AFI16-1401, 29 July 2019

Pages: 12

This publication implements Air Force Policy Directive (AFPD) 16-14, *Security Enterprise Governance*. It provides guidance and procedures for the oversight, management and execution of information protection programs, throughout the Department of the Air Force (DAF). It 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 to the office of primary responsibility (OPR) listed above, using the Department of the Air Force (DAF) Form 847, *Recommendation for Change of Publication*, and route through your local information protection office. This publication applies to all civilians and uniformed members of the Regular Air Force, United States Space Force (USSF), Air Force Reserve, Air National Guard, the Civil Air Patrol (when conducting missions as the official Air Force Auxiliary), and those with a contractual obligation to abide by the terms of DAF issuances. The authorities to waive requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See Department of the Air Force Manual (DAFMAN) 90-161, *Publishing Processes and Procedures,* for a description of the authorities associated with the Tier numbers.

Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction (AFI) 33-322, *Records Management and Information Governance Program,* and are disposed of in accordance with the Air Force Records Disposition Schedule, which is in the Air Force Records Information Management System. 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 DAF.

SUMMARY OF CHANGES

Removes the requirement for activities to use the Enterprise Protection Risk Management (EPRM) tool, as the system of record, to complete the Information Security Oversight Office (ISOO) annual self-inspection report and documenting security compliance inspections. Incorporates the controlled unclassified information (CUI) program under the information protection program umbrella. In Section 2 – "Roles and Responsibilities," guidance applies to all United States Space Force (USSF), Headquarters Air Force (HAF), and Secretary of the Air Force (SAF) equivalents.

1. Purpose of the Information Protection Program. To develop policy and an integrated security framework and strategic plan for the management and oversight of the information protection program, which consists of the controlled unclassified information (CUI), and the industrial, information, and personnel security programs. This framework aligns with the requirements identified in DoDD 5200.43, *Management of Defense Security Enterprise*.

2. Roles and Responsibilities.

2.1. Administrative Assistant to the Secretary of the Air Force (SAF/AA). Serves as the DAF senior agency official (SAO) and security program executive (SPE).

2.1.1. The Director, Security, Special Program Oversight and Information Protection (SAF/AAZ):

2.1.1.1. Develops policy and guidance for security disciplines under the information protection program and oversees implementation.

2.1.1.2. Serves as the DAF focal point for the counter-insider threat program in accordance with Headquarters Air Force (HAF) Mission Directive 1-6, *Administrative Assistant to the Secretary of the Air Force*.

2.1.1.3. Manages and oversees the information protection core security disciplines for the DAF inspection system, to support operational planning and mission execution in accordance with AFI 90-201, *Air Force Inspection System*. Continuously evaluates trends for potential changes in policy, training, assessments, and inspections.

2.1.1.4. Administers the DAF CUI program.

2.1.2. The Director, Information Management (SAF/AAI). Governs the DAF declassification programs, which consists of automatic, systematic, and National Archives declassification review programs as well as the mandatory declassification review program.

2.2. Assistant Secretary of the Air Force for Acquisition, Technology and Logistics (SAF/AQ).

2.2.1. Develops policy and procedures for implementing security requirements into solicitations, contracts, and other transactions, in support of the National Industrial Security Program.

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

2.2.3. Produces policies and guidance for science, technology, and program protection that incorporate methodologies and techniques to identify and protect research, developmental, and fielded system information, components, processes, and technologies.

2.3. Chief Information Officer (SAF/CN).

2.3.1. Serves as the DAF Chief Information Officer, charged with carrying out DAF's responsibilities for information resources management, information technology, information security, and national security systems under 44 USC § 3506, *Federal Agency Responsibilities;* 44 USC § 3554, *Federal Agency Responsibilities;* 40 USC § 11315, *Agency Chief Information Officer*; and 10 USC § 2223, *Information technology: additional responsibilities of Chief Information Officers* as implemented by the Department of Defense (DoD).

2.3.1.1. SAF/CNZ serves as the Chief Information Security Officer, charged with overseeing, developing, and executing the DAF cybersecurity program.

2.3.2. Provides policy and recommendations to SAF/AA on updates for the sharing, marking, safeguarding, storage, dissemination, decontrol, destruction, and records management of DAF CUI residing on both DoD and non-DoD information systems, in accordance with DoDI 8582.01, *Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information* and DoDI5200.48_DAFI16-1403, *Controlled Unclassified Information*.

2.4. Assistant Secretary of the Air Force for International Affairs (SAF/IA).

2.4.1. Directs, administers, and oversees the DAF foreign disclosure program, which consists of, safeguarding foreign government or representative information. Approves the disclosure of classified information and CUI to foreign governments or representatives and international organizations. Manages disclosure arrangements for international programs and foreign visits.

2.4.2. On behalf of SAF/IA, the Air Force Life Cycle Management Center (AFLCMC) oversees all aspects of international program security and will coordinate with SAF/AAZ to develop and disseminate information protection policy and procedures pertaining to security cooperation.

2.4.2.1. Director, Air Force Security Assistance & Cooperation. Serves as the DAF security cooperation program management lead for security and information protection. The AFLCMC ensures recipient foreign governments and/or representatives have both the capability and intent to protect classified information and materials, and CUI, to the equivalent U.S. government standards.

2.5. Deputy Chief of Staff, Manpower, Personnel and Services (AF/A1) Directorates:

2.5.1. Director, Civilian Force Management (AF/A1C). Oversees implementation and sustainment of civilian personnel policies for all DAF Title 5 and Title 10 civilian personnel systems and programs.

2.5.2. Director, Manpower, Organization, and Resources (AF/A1M).

2.5.2.1. Defines DAF manpower requirements and managing corporate DAF manpower and personnel programming and resource distribution for the total force, while ensuring corporate DAF manpower requirements link mission capabilities to programmed resources.

2.5.2.2. Notifies SAF/AAZ of changes to manpower and career field requirements that will impact the personnel security investigation's budget and/or any other emerging programs impacting budget and resources of information protection, on a semi-annual basis.

2.6. Assistant Secretary of the Air Force for Manpower and Reserve Affairs (SAF/MR). Serves as an agent of the Secretary and provides guidance, direction, and oversight for Homeland Security Presidential Directive-12, *Suitability and Fitness Program*. Oversees the Personnel Security Appeal Board and renders final appeal decisions on security clearance denials and/or revocation.

2.7. Deputy Chief of Staff, Intelligence, Surveillance, Reconnaissance, and Cyber Effects Operations (AF/A2/6). Responsible for the oversight, management, and administration of the sensitive compartmented information program.

2.8. Deputy Chief of Staff, Strategic Deterrence and Nuclear Integration (AF/A10).

2.8.1. Serves as the DAF restricted data management official, for the nuclear information security program.

2.8.2. Serves as the principal advisor to the DAF Restricted Data Management Official (SAF/AA).

2.8.3. Serves as the DAF lead for access to Department of Energy (DOE) sigma nuclear weapon data.

2.8.4. Serves as the DAF OPR for the classification and declassification of DAF information marked restricted data or formerly restricted data and coordinates changes with Assistant Secretary of Defense for Nuclear, Chemical & Biological Defense Programs, as necessary.

2.9. Commander, Headquarters United States Air Forces in Europe – Air Force Africa (USAFE-AFAFRICA). Serves as the DAF Executive Agent for the North Atlantic Treaty Organization (NATO) program. The USAFE-AFAFRICA Director, Information Protection functions as the program manager and represents the DAF at NATO meetings and interagency forums, and forwards requests to establish and/or disestablish NATO sub-registries, within the DAF, to the Central United States Registry.

2.10. Commander, Air Combat Command. Serves as the DAF sanitization lead for classified collateral data spillages and classified message incident reporting, via the Sixteenth Air Force.

2.11. Major Command (MAJCOM), Field Command (FLDCOM), Direct Reporting Unit (DRU), and Forward Operating Agency (FOA) Commanders/Directors appoint SPEs at a level no lower than vice commander (CV) or deputy commander (CD).

2.12. SPE, MAJCOM, FLDCOM, DRU, and FOA.

2.12.1. Administers and oversees the information protection programs by enforcing adherence to prescribed security standards.

2.12.2. Implements a mandatory declassification review program.

2.12.3. Collaborates with the Director, Information Protection to integrate the core security disciplines into command operations, to help ensure consistent compliance and risk management through standardized guidelines, inspections, regulations, and other measures.

2.13. MAJCOM, FLDCOM, DRU, and FOA Director, Information Protection.

2.13.1. Administers the information protection program, on behalf of the CV or CD, and develops guidance for program implementation within activity operations.

2.13.2. Provides oversight, direction, and training to staff security specialists for the efficient and effective implementation of the information protection programs.

2.13.3. Delivers program management, oversight, and risk management policy and guidance to subordinate units.

2.14. Wing, Delta or Installation Commanders.

2.14.1. Provide direct oversight for implementing the DAF information protection programs by ensuring security controls, safeguards, and countermeasures are established through application of risk management principles, as appropriate, for their wing/delta and tenant organizations residing on their installations when documented in support agreements; this may be delegated to the CV or CD. Tenant organization commanders, with a dedicated activity security manager, may opt to maintain independent oversight of their information protection programs. A host installation's information protection office may not deny or terminate a DAF tenant organization's supporting cognizant security office (CSO) relationship without the coordination and approval of the tenant's parent CSO.

2.14.2. Appoint a Chief, Information Protection (CIP) who resides on the wing/delta special staff and makes sure he/she has a clear line of reporting to the CV or CD, for any information protection security matters. Hiring an individual into an authorized funded position designated as a CIP, serves as an appointment.

2.15. Chief, Information Protection (CIP).

2.15.1. In executing the command's information protection program, functions as the commander's principal advisor for security matters.

2.15.2. Serves as the activity security manager for the wing/delta (installation). More specific roles and responsibilities are defined in enclosure 2 of DoDM5200.01V1_DAFMAN16-1404V1, *Information Security Program*: *Overview, Classification, and Declassification*.

2.15.3. Establishes, develops, coordinates, and implements DAF security enterprise activities, policies and procedures for the oversight, execution, management, risk management, and administration of these core security disciplines.

2.15.4. Validates completion of annual self-assessment checklists (SACs), in the Management Internal Control Toolset (MICT). This includes, identifying when an activity is performing well or in need of assistance to accomplish its mission and communicating with command leadership on the health of the core security disciplines, as needed.

2.15.5. Reviews supplemental core security discipline instructions, processes and procedures for compliance with prescribed policy requirements.

3. Self-Assessments and Compliance Inspections.

3.1. Annual compliance inspections consist of the information protection office analyzing the supported activity's security metrics, data systems, inspection reports, inventory controls, requests for assistance, and MICT SACs, to evaluate compliance.

3.2. Commanders/directors must ensure annual self-assessments and program inspections, are completed, as required. This includes monitoring deficiencies and continually evaluating mission and inspection readiness. **Note**: Annual ISOO or Under Secretary of Defense for Intelligence and Security reports and/or data calls do not supplant this requirement.

3.3. The EPRM tool is no longer the system of record for conducting annual self-assessments or program compliance inspections. This function will be administered through MICT and the Inspector General Evaluation Management System (IGEMS). **(T-1)**

4. Security Education and Training.

4.1. Commanders/directors will ensure all assigned personnel are educated on their roles and requirements in support of security policies, processes, and procedures, and complete all mandatory security training, as outlined in enclosure 5, of DoDM5200.01V3_DAFMAN16-1404V3, *Information Security Program: Protection of Classified Information* and chapter 5, of AFI 36-2645, *Security Professional Certification and Development*, at minimum. **(T-0)**

4.2. Individuals with specified duties in the information protection programs must be provided security education opportunities and training commensurate with job responsibilities that is sufficient to permit effective performance of those duties. Individuals in appointed positions must meet prescribed training requirements no later than six months from appointment, unless otherwise specified. **(T-0)**

ANTHONY P. REARDON, SES, DAF
Administrative Assistant

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

44 USC § 3506, *Federal Agency Responsibilities*

44 USC § 3554, *Federal Agency Responsibilities*

40 USC § 11315, *Agency Chief Information Officer*

10 USC § 2223, *Information Technology: Additional Responsibilities of Chief Information Officers*

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

Executive Order 13556, *Controlled Unclassified Information,* 4 November 2010

Homeland Security Presidential Directive-12, *Suitability and Fitness Program*

DoDD 5200.43, *Management of Defense Security Enterprise,* 14 July 2020

DoDI 8582.01, *Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information,* 9 December 2019

AFPD 16-14, *Security Enterprise Governance*, 31 December 2019

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

DAFMAN 90-161, *Publishing Processes and Procedures*, 15 April 2022

AFI 33-322, *Records Management and Information Governance Program*, 23 March 2020

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

AFI 36-2645, *Security Professional Certification and Development,* 11 June 2020

DoDM5200.01V1_DAFMAN16-1404V1, *Information Security Program*: *Overview, Classification, and Declassification*, 6 April 2022

DoDM5200.01V3_DAFMAN16-1404V3, *Information Security Program: Protection of Classified Information*, 12 April 2022

DoDI5200.48_DAFI16-1403, *Controlled Unclassified Information*, 5 October 2021

DoDM5200.02_DAFMAN16-1405, *Air Force Personnel Security Program,* 1 August 2018

Prescribed Forms

None

Adopted Forms

DD Form 254, *Department of Defense Contract Security Classification Specification*

DAF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AFI—Air Force Instruction

AFLCMC—Air Force Lifecycle Management Command

AFPD—Air Force Policy Directive

CC—commander

CD—deputy commander

CIP—Chief, Information Protection

CSO—cognizant security office

CUI—controlled unclassified information

CV—vice commander

DAF—Department of the Air Force

DAFI—Department of the Air Force Instruction

DAFMAN—Department of the Air Force Manual

DoD—Department of Defense

DoDI—Department of Defense Instruction

DoDM—Department of Defense Manual

DOE—Department of Energy

DRU—Direct Reporting Unit

EPRM—Enterprise Protection Risk Management [tool]

FLDCOM—field command

FOA—Forward Operating Agency

HAF—Headquarters Air Force

IGEMS—Inspector General Evaluation Management System

IP—Information Protection

ISOO—Information Security Oversight Office

MAJCOM—major command

MICT—Management Internal Control Toolset

NATO—North Atlantic Treaty Organization

OPR—office of primary responsibility

SAF—Secretary Air Force

SAC—self-assessment checklist

SecAF—Secretary of the Air Force

SPE—Security Program Executive

SAO—Senior Agency Official

U.S.—United States

USSF—United States Space Force

Office Symbols

AF/A1—Deputy Chief of Staff, Manpower, Personnel and Services

AF/A1C—Director, Civilian Force Management Directorate

AF/A1M—Manpower, Organization and Resources Directorate

AF/A2/6—Deputy Chief of Staff, Intelligence, Surveillance, Reconnaissance, and Cyber Effects Operations

AF/A4—Deputy Chief of Staff, Logistics, Engineering and Force Protection

AF/A10—Deputy Chief of Staff, Strategic Deterrence and Nuclear Integration

AFLCMC—Air Force Life Cycle Management Center

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

SAF/AAZ—Security, Special Program Oversight and Information Protection Directorate

SAF/AAI—Information Management Directorate

SAF/AQ—Assistant Secretary of the Air Force for Acquisition, Technology and Logistics

SAF/CN—Chief Information Officer

SAF/CNZ—Chief Information Security Officer

SAF/IA—Assistant Secretary of the Air Force for International Affairs

SAF/MR—Assistant Secretary of the Air Force for Manpower and Reserve Affairs

USAFE-AFAFRICA—Headquarters United States Air Forces in Europe – Air Force Africa

Terms

Activity Security Manager—The individual specifically designated in writing and responsible for the installation's information protection program. An example of an activity security manager is the installation Chief, Information Protection, or any members of their staff. This term may also be associated with an organization where the commander/director opts out of host installation information protection support, as administered in accordance with a support agreement. In order to opt out an organization must establish its own IP Office with all the capabilities and functionality of an IP Office and must be provided IP oversight by the appropriate higher headquarters.

Assistant Security Manager—A U.S. government civilian or military member designated, in writing, to assist the activity security manager with implementation, maintenance and oversight of the security program.

Controlled Unclassified Information (CUI)—Unclassified information requiring safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and government-wide policies. Some CUI may also be export-controlled or protected by contract.

Information Protection—Is a subset of the DAF Security Enterprise. Information Protection consists of a set of three core security disciplines (Personnel, Industrial, and Information Security) used to:

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

Ensure the protection of classified information that may be released or has been released to current, prospective, or former contractors, licensees, or grantees of U.S. agencies.

Protect classified information that, if subject to unauthorized disclosure, could reasonably be expected to cause damage to national security. Protect CUI, which may be withheld from release to the public.

Inspector General Evaluation Management System (IGEMS)—IGEMS (to include the classified version) facilitates scheduling, planning, inspecting, and report writing for inspector general inspections. IGEMS is also used to assign, monitor, and close (if applicable) all findings (strengths, recommended improvement areas, deficiencies) identified during the inspection process. The system is comprised of an open architecture which facilitates manual enterprise-level trending analysis and cross communication with normalized data and standardized reporting.

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, *Classified National Security Information* 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 controlled unclassified information, which may be withheld from release to the public in accordance with statute, regulation, or policy.

Management Internal Control Toolset (MICT)—MICT is a DAF program of record and provides units a tool for managing their self-assessment programs. It also provides a means to communicate a unit's program health. MICT also provides supervisors and the command chain (from squadron commander to SecAF) tiered visibility into user-selected compliance reports and program status as well as indications of program health across functional and command channels.

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 DoD, 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.

Risk Management—The process of identifying, assessing, and controlling risks and making decisions that balance risk with cost and benefits.

Security—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. More specifically, proactive measures adopted to safeguard personnel, information, operations, resources, technologies, facilities, and foreign relations against harm, loss, or hostile acts and influences.

Security Assistant—Security assistants are U.S. government civilian or military personnel who perform administrative security functions, under the direction of their commander/director and oversight of an activity security manager. An example of a security assistant is an individual with the commander's support staff, who is trained in accordance with the scope and complexity of the organization's mission, to generate periodic reinvestigation reports and document access in Defense Information Security System (or successor system), and record non-disclosure agreement completion.

Security Enterprise—The framework for integrating the personnel security, industrial security, information security, physical security, operations security, special access program security, critical program information protection, and security training.

Security Enterprise Management Support—Enhance support to operational mission readiness, Information Protection should increase coordination/integration with operational planners, foreign disclosure office, special access program, and cybersecurity entities to inject information protection elements into security planning into daily and ongoing missions, such as operations security plans, release determinations, and system vulnerabilities.

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 SPE shall be accountable for credible cost, schedule, and performance reporting to the Defense Security Executive. At the HAF, this is SAF/AA; at the MAJCOM, FLDCOM, DRU, and FOA, this is the vice (or deputy) commander.

Security Specialist—Civilian personnel in the Office of Personnel Management occupational series 0080, *Security Administration,* or military personnel assigned security functions as an additional duty. They are responsible for implementing information protection core security disciplines.

Self-Assessment Checklist (SAC)—A SAC is a list of available questions which allows communication to commanders at each level, within the wing/delta construct, designed to assess compliance based upon commander's intent and direction for the organization. In addition, those SACs generated by HAF or a MAJCOM, FLDCOM, DRU, and FOA, provides indicators to the functional community, allowing for a more in-depth understanding of policy effects on wing/delta and below organizations.

Senior Agency Official—An official appointed by the head of a DoD component to be responsible for direction, administration, and oversight of the security enterprise, to include classification, declassification, safeguarding, and security education and training programs, and for the efficient and effective implementation.