BY ORDER OF THE
SECRETARY OF THE AIR FORCE

DEPARTMENT OF THE AIR FORCE
INSTRUCTION 16-1401

3 FEBRUARY 2023

AIR FORCE RESERVE COMMAND
Supplement

11 SEPTEMBER 2025

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: 18

(AFRC)

OPR: HQ AFRC/IP

Certified by: HQ AFRC/IP

Pages: 6

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.

(AFRC) DAFI 16-1401, *Information Protection Program*, is supplemented as follows: This supplement applies to all civilians and uniformed members of the Air Force Reserve Command (AFRC) at AFRC installations. It is not applicable to AFRC tenants on other MAJCOM installations, the Air National Guard, Regular Air Force, or the United States Space Force. This supplement provides guidance and procedures for the oversight, management and execution of information protection programs, throughout AFRC. 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. 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. Submit requests for waivers through the chain of command to the appropriate tier waiver approval authority, or alternately, to the publication OPR for non-tiered compliance items. 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 (AFRIMS). 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*.

1. (AFRC) Purpose of the Information Protection Program. This framework also includes the counter-insider threat program.

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).

2.11. **(AFRC)** AFRC/CD is the SPE.

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.

2.14.1. **(AFRC)** Assures IP program requirements are integrated into all facets of mission/deployment/basing action planning, agreement development, execution and coordination affecting all assigned and tenant personnel, resources and weapon platforms.

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.

2.15.4. **(AFRC)** The CIP evaluates SACs and quarterly random entry/exit inspections procedures during annual unit compliance inspections. Provide commanders with a written inspection report within 30 calendar days of completing the annual unit compliance

inspection. **(T-2)** Coordinate with the local IGI for access to IGEMS for standardized reporting and deficiency tracking.

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

2.15.6. **(Added-AFRC)** The CIP validates all contractor requests for access to classified National Security information on their installations via the DD Form 254, *Department of Defense Contract Security Classification Specification*. They ensure there is a contract relationship with a Government organization on the installation and there is a Government representative on-site to oversee contractor operations. All unsolicited requests for access to information and IT systems from contractor employees will be reported the Defense Counterintelligence and Security Agency Cognizant Security Office listed on the DD Form 254. **(T-2)**

2.16. **(Added-AFRC)** Air Force Reserve Command.

2.16.1. **(Added-AFRC)** HQ AFRC Information Protection (IP) Directorate Program Managers, Activity Security Managers, Assistant Security Managers, and Security Assistants are authorized to randomly sample classified documents/equipment, commensurate to their clearance eligibility and access, to ensure documents are properly marked in in accordance with enclosure 3 of DoDM 5200.01V2_DAFMAN16-1404V2, *DoD Information Security Program: Marking of Information*. **(T-0)** This sampling includes classified documents supporting Restricted Data/Formerly Restricted Data, NATO and Foreign Government Information, and Nuclear Command and Control-Extremely Sensitive Information programs. This authority does not extend to Special Access Program, Sensitive Compartmented Information, or COMSEC documents/equipment.

2.16.2. **(Added-AFRC)** AFRC IP Offices shall not exercise the role of the primary or alternate Mission Partner Identity, Credentialing, and Access Management, Installation Point of Contact, Mission Partner Affiliation Security Manager, Mission Partner Affiliation Sponsor, Super Verifying Official, Verifying Official, Issuing Official, Local Registration Authority, Site Security Manager, or the role of the signatory sponsor on the DD Form 1172-2, *Application for Identification Card/DEERS Enrollment*. **(T-2)** To maintain separation of duties with Industrial Security program management and inspection oversight responsibilities, the IP Office merely assists commanders, and their security assistants, in validating the status of applicant background investigations and fingerprint checks in accordance with DoDM 1000.13-M-V1, *DoD Identification (ID) Cards: ID Card Life-Cycle*, and DAFMAN 36-3026, *Mission Partner Identity, Credentialing, and Access Management.*

2.16.3. **(Added-AFRC)** Security Containers.

2.16.3.1. **(Added-AFRC)** Safe/security container, open storage area/secure room and vault custodian appointments are not required. Annotations in block 11 of the Standard Form (SF) 700, *Security Container Information,* Part 1, identify who is responsible for the container, area, room or vault.

2.16.3.2. **(Added-AFRC)** Use SF 700, Part 2, to record the combination is not required unless determined by commander for emergencies. Discard the Part 2, unless it is used to record the combination.

2.16.3.3. **(Added-AFRC)** Risk assessments are not required for GSA-approved security containers storing Secret and below information/material.

2.16.4. **(Added-AFRC)** "Secure spaces" and "classified spaces" are defined as collateral vaults and open storage areas/secure rooms approved in accordance with DoDM 5200.01V3_DAFMAN16-1404V3, and those areas (determined by the installation commander) processing or storing significant amounts of classified information. Spaces where classified information is processed on classified IT systems are also referred to as Classified Processing Areas (CPAs) in accordance with the AF Emission Security (TEMPEST) program. Both programs (IP and TEMPEST) have their own approval processes—the IP Office owns the process for approving vaults and open storage areas/secure rooms; the TEMPEST program manager owns the process for approving CPAs.

2.16.4.1. **(Added-AFRC)** For CPAs not located inside of a collateral vault or open storage area/secure room approved in accordance with DoDM 5200.01V3_DAFMAN16-1404V3, the IP Office assists the TEMPEST program manager by ensuring IP program requirements are met. The IP program manager will provide TEMPEST program manager with requested artifacts to approve the TEMPEST package.

2.16.4.2. **(Added-AFRC)** For CPAs located in a collateral vault or open storage area/secure room approved in accordance with DoDM 5200.01V3_DAFMAN16-1404V3, IP program manager must approve the vault or open storage area/secure room before the TEMPEST program manager can approve the TEMPEST package.

2.16.4.3. **(Added-AFRC)** See DAFMAN 17-1301, *Computer Security*, paragraph 4.2. for guidance on general protection requirements necessary to support AFSSI 7700, *Emissions Security*, requirements for TEMPEST packages.

2.16.5. **(Added-AFRC)** Quarterly Random Entry/Exit Inspections of Collateral Secure Spaces. Commanders will:

2.16.5.1. **(Added-AFRC)** Identify in local policy applicable secure spaces subject to these quarterly random entry/exit inspections. **(T-2)**

2.16.5.2. **(Added-AFRC)** The inspection frequency may be increased at the installation commander's direction.

2.16.5.3. **(Added-AFRC)** For maximum effect, inspection schedules will not be advertised or released in advance. **(T-2)**

2.16.5.4. **(Added-AFRC)** Inspection times should include consideration of personnel reporting to work before and remaining after scheduled duty hours.

2.16.5.5. **(Added-AFRC)** Commanders appoint owner/user personnel to complete random entry/exit inspections. IP Office staff will not be tasked to conduct these inspections. **(T-2)**

2.16.6. **(Added-AFRC)** Commanders will ensure the alpha personnel rosters for military and civilian members are reviewed and cross referenced with the Defense Information System for Security (DISS) subject report bi-monthly to ensure accurate and positive ownerships of individuals in the system of record. **(T-0)** They will provide the IP Office a listing of all relationship changes made for individuals in DISS. **(T-2)**

2.16.7. **(Added-AFRC)** Personnel Security Vetting Actions.

2.16.7.1. **(Added-AFRC)** The IP office is not responsible for initiating personal vetting actions of new civilian hires or new military accessions. This includes, but is not limited to, responding to Defense Counterintelligence and Security Agency supplemental information requests or initial personnel vetting questionnaire submittals for security clearance processing. **(T-2)** IP offices shall not establish an owning or servicing relationship in DISS while the new member is on boarding, in a delayed entry program, or prior to successful completion of Air Force Basic Military Training and/or graduated from their assigned technical school.

2.16.7.2. **(Added-AFRC)** Personnel Vetting Questionnaire updates (formerly SF 86, *Questionnaire for National Security Positions,* updates) must be completed in the National Background Investigation Services electronic application and forwarded to the IP Office within 14 calendar days of the member being notified. **(T-2)** These updates do not require the covered member to be on a unit training assembly, annual tour, or other pay status. Extensions may be granted (in writing) due to extenuating circumstances for an additional 14 calendar days by the member's commander. **(T-2)** All covered members who fail to complete updates within the prescribed timelines are subject to local suspension of access and Continuous Evaluation incident reporting.

2.16.8. **(Added-AFRC)** Reporting Misuse/Unauthorized Disclosures (UD) of Controlled Unclassified Information (CUI).

2.16.8.1. **(Added-AFRC)** If disciplinary action is not expected to be taken against the individual(s) responsible for the misuse or UD of CUI, the commander must promptly chronical the events which caused the misuse/UD in a memorandum. **(T-2)** The memorandum must include a synopsis of all relevant facts concerning the incident and appropriate changes made, actions taken, or training provided to correct or eliminate the conditions contributing to the incident. This action is required in addition to any other mandated, corresponding program reporting requirements.

2.16.8.2. **(Added-AFRC)** If disciplinary action is expected to be taken against the individual(s) responsible for the misuse or UD of CUI, the commander must appoint an inquiry official, in writing, within three (3) duty days from the discovery of the misuse/UD. **(T-2)** Every attempt should be made to ensure these officials are equal to, or higher in rank/grade, than the suspected culpable parties involved in the incident. Inquiry officials will not be a person assigned to the IP Office. **(T-2)** Document the Misuse/UD of Controlled Unclassified Information Report similar to the Security Incident Reporting Format at Appendix 1 to Enclosure 6, of DoDM 5200.01V3_DAFMAN16-1404V3. **(T-2)** The report must include a synopsis of all relevant facts concerning the incident and appropriate changes made, actions taken, or training provided to correct or eliminate the conditions contributing to the incident.

This action is required in addition to any other mandated, corresponding program reporting requirements.

2.16.8.3. **(Added-AFRC)** Regardless of the conditions noted above, the matter must be initiated and completed within 10 duty days. **(T-2)** The completed Misuse/Unauthorized Disclosure of Controlled Unclassified Information Report must be closed by the commander who appointed the inquiry official. The commander will provide a copy of the closed report to IP Office. Extensions to this timeline are at the discretion of the commander, with consultation of the IP Office and other program subject matter experts affected by the misuse/UD.

2.16.8.4. **(Added-AFRC)** Maintain the Misuse/Unauthorized Disclosure of Controlled Unclassified Information Reports in accordance with AFRIMS, Table 31-04, Rule 13.00 (or subsequent revisions). **(T-1)**

2.16.9. **(Added-AFRC)** The content of local security policy communicated to contractor visitor groups is determined locally. This policy may include other security program information contributed by other subject matter experts. Codify this policy in the DD Form 254, an attachment to the form, or as a separate enclosure/memorandum. **(T-2)**

2.16.10. **(Added-AFRC)** Commanders hosting contractors requiring access to classified information must maintain the following documentation, and present this documentation for inspection upon request: DD Form 254, Visit Notification(s) (maintained in DISS), list of Key Management Personnel (for Cleared Facilities), and a copy of the local security policy if not in the DD Form 254, or an attachment to the form. **(T-2)**

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.

3.1. **(AFRC)** Annual IP program compliance inspections may count as a self-assessment for an organization.

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.

3.2. **(AFRC)** Organizations who do not possess or store collateral classified information/material may be inspected biennially instead of annually, as determined by the installation commander. This determination may be delegated no lower than the Chief of Information Protection.

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)**

4.3. **(Added-AFRC)** The following Information Protection training must be completed and accounted for in the MyLearning platform. **(T-2)** If a course is removed from MyLearning's library, and is still mandated, collaborate with the Wing's Training Manager to account for and track the training locally within MyLearning. Refer to the corresponding guidance for the frequency of each training requirement and the Wing Training Manager for approved alternatives for delivering this training.

4.3.1. **(Added-AFRC)** *DoD Initial Orientation & Awareness Training course* (DoDM 5200.01V3_DAFMAN16-1404V3, Enclosure 5, para 3)

4.3.2. **(Added-AFRC)** *DoD Annual Security Refresher Training course* (DoDM 5200.01V3_DAFMAN16-1404V3, Enclosure 5, para 7)

4.3.3. **(Added-AFRC)** *Derivative Classification course* (DoDM 5200.01V3_DAFMAN16-1404V3, Enclosure 5, para 7c & 7g)

4.3.4. **(Added-AFRC)** *DoD Mandated Controlled Unclassified Information (CUI) Training course* (DoDI 5200.48_DAFI16-1403, Sections 2.10d & 3.6b)

4.3.5. **(Added-AFRC)** *Insider Threat Awareness course* (DAFI 16-1402, *Counter-Insider Threat Program Management,* para 3.3)

4.4. **(Added-AFRC)** The *Initial Access Briefing* (DoDM 5200.01V3_DAFMAN16-1404V3, Enclosure 5, para 3c) must be completed by all personnel granted access to classified information. **(T-0)** Written acknowledgements of these briefings will be presented upon request.

4.5. **(Added-AFRC)** The *NATO Briefing* acknowledgement (DoDM 5200.01V1_DAFMAN16-1404V1, Enclosure 3, para 12c) must be completed by all personnel granted access to classified information IT systems. **(T-0)** Written acknowledgements of these briefings will be presented upon request.

4.6. **(Added-AFRC)** In accordance with DoDM 5200.02_DAFMAN16-1405, Section 11.2a(a), personnel assigned to sensitive duties, or granted security clearance eligibility, and/or have been granted access to classified information, must be briefed annually on the national security implications of their duties and their individual responsibilities. **(T-0)** The *Receive and Maintain Your National Security Eligibility* tool at the link below, and Intelligence Community Policy Guidance (ICPG) 704.2., *Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Programs,* may be used to satisfy this briefing requirement. If local products are developed for use to satisfy this mandate, ensure these products emphasize the individuals' responsibility to meet the standards and criteria for security eligibility as identified

in ICPG 704.2. Written acknowledgements of this briefing will be presented upon request. **https://www.cdse.edu/Portals/124/Documents/jobaids/personnel/Receive_and_Maint_Sct_Clnc.pdf**

4.7. **(Added-AFRC)** Access to classified IT systems, and authority to derivatively classify information, may only be granted upon confirmation all training requirements and briefings identified in paragraphs **4.3** through **4.5** have been completed. **(T-0)** When annual and refresher training requirements lapse, access to classified IT systems must be suspended unless specific requirements are appropriately waived in accordance with DoDM 5200.01V3_DAFMAN16-1404V3, Enclosure 5. **(T-0)**

ANTHONY P. REARDON, SES, DAF
Administrative Assistant

(AFRC)

REGINA A. SABRIC
Major General, USAF
Deputy Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

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

40 USC § 11315, *Agency Chief Information Officer*

44 USC § 3506, *Federal Agency Responsibilities*

44 USC § 3554, *Federal Agency Responsibilities*

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

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

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

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

(Added-AFRC) AFSSI 7700, *Emissions Security*, 14 April 2009

(Added-AFRC) DAFI 16-1402, *Counter-Insider Threat Program Management*, 10 May 2024

(Added-AFRC) DAFMAN 17-1301, *Computer Security,* 9 December 2024

(Added-AFRC) DAFMAN 36-3026, *Mission Partner Identity, Credentialing, and Access Management*, 15 August 2024

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

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

(Added-AFRC) DoDI 5200.48_DAFI16-1403, *Controlled Unclassified Information (CUI)*, 5 October 2021

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

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

(Added-AFRC) DoDM 1000.13-M-V1, *DoD Identification (ID) Cards: ID Card Life-Cycle*, 23 January 2014

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

(Added-AFRC) DoDM 5200.01V2_DAFMAN16-1404V2, *DoD Information Security Program: Marking of Information*, 7 January 2021

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

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

(Added-AFRC) DoDM 5220.22V2_DAFMAN16-1406V2, *National Industrial Security Program: Industrial Security Procedures for Government Activities*, 8 May 2020

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

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

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

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

(Added-AFRC) ICPG 704.2., *Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Programs*, 2 October 2008

Prescribed Forms

None

(Added-AFRC) None

Adopted Forms

(**Added-AFRC**) DD Form 1172-2, *Application for Identification Card/DEERS Enrollment*

DD Form 254, Department of Defense Contract Security Classification Specification

DAF Form 847, *Recommendation for Change of Publication*

(**Added-AFRC**) SF 700, *Security Container Information*

(**Added-AFRC**) SF 86, *Questionnaire for National Security Positions*

Abbreviations and Acronyms

AFI—Air Force Instruction

AFLCMC—Air Force Lifecycle Management Command

AFPD—Air Force Policy Directive

(Added-AFRC) AFRC—Air Force Reserve Command

(Added-AFRC) AFRIMS—Air Force Records Management Information Security

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

(Added-AFRC) DISS—Defense Information System for Security

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

(Added-AFRC) TEMPEST—Transient Electro-Magnetic Pulse Emanation Standard

U.S.—United States

(Added-AFRC) UD—Unauthorized Disclosures

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

(Added-AFRC) AFRC/IP—Directorate of Information Protection

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.