BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE POLICY DIRECTIVE 16-14

31 DECEMBER 2019

Operations Support

SECURITY ENTERPRISE GOVERNANCE

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)

Supersedes: AFPD 16-14, 24 Jul 14

Pages: 11

This publication implements Department of Defense (DoD) Directive (DoDD) 5200.43, *Management of the Defense Security Enterprise*; DoDD 5210.50, *Management of Serious Security Incidents Involving Classified Information*; DoDD 5205.16, *The DoD Insider Threat Program*; DoD Instruction (DoDI) 5200.01, *DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI);* DoDI 5200.02, *DoD Personnel Security Program (PSP);* and DoDI 5220.22, *National Industrial Security Program (NISP).* This policy directive applies to all civilian employees and uniformed members of the Regular Air Force, Air Force Reserve, and Air National Guard, contractors and consultants (when contract performance supports the functions listed in this policy directive). Refer recommended changes and questions about this publication to the Office of Primary Responsibility using the Air Force (AF) Form 847, *Recommendation for Change of Publication*; route the AF Form 847 from the field through the appropriate functional chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AF Manual 33-363, *Management of Records*, and disposed of in accordance with AF Records Disposition Schedule located in the AF Records Information Management System.

SUMMARY OF CHANGES

This publication has been substantially revised and must be reviewed in its entirety. Major changes include the removal of Attachment 2 and the inclusion of AF/A1 and SAF/MR suitability and fitness roles and responsibilities. Other changes comprise of the revision of roles and responsibilities for other Secretariat of the Air Force (SAF) and Headquarters Air Force (HAF) organizations impacted by the updated DoD Insider Threat policy as well as the transfer

of previously assigned Insider Threat Program roles and responsibilities to SAF and HAF organizations from its previous location in the AF Instruction 16-1402, *Insider Threat Program Management,* and the AF Guidance Memorandum to the Instruction. Additionally, revisions to organizational name changes attributed to HAF reorganization and overall reformatting to comply with current publication guidance.

1. Overview. The AF Security Enterprise is the framework for integrating personnel security, industrial security, information security, physical security, operations security, special access program security, critical program information protection, and security training. This framework aligns with counterintelligence, intelligence, information operations, foreign disclosure, security cooperation, technology transfer, export control, cybersecurity, nuclear physical security, chemical and biological agent security, antiterrorism, force protection, and mission assurance, and is informed by other security-related efforts.

2. Policy. The AF will:

2.1. Implement standardized security processes, to the maximum extent possible, with appropriate provisions for unique missions and security environments to ensure maximum interoperability, consistent quality assurance and cost efficiencies.

2.2. Ensure functional leads within their respective Mission Directive-assigned authorities and responsibilities collaborate on resource requirements, risk management, policy integration, personnel training and other areas impacting the Air Force Security Enterprise.

2.3. Use the Air Force Security Enterprise Executive Board to provide an enterprise-wide, integrated organizational perspective to the security enterprise policy development, risk management, resource advocacy, oversight, implementation and training.

2.4. Implement the standards for Executive Branch Insider Threat Programs listed in the Presidential Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, in accordance with the DoD implementation plan prescribed in DoDD 5205.16.

2.5. Ensure appropriate security controls, safeguards, and countermeasures are established, implemented, and applied to address risk specific to each installation to an acceptable level.

2.6. Execute the Air Force Information Security Program consistent with DoDD 5210.50 and DoDI 5200.01. The Information Security program will assure the protection of collateral classified, Sensitive Compartmented Information, Special Access Program Information, and Controlled Unclassified Information.

2.7. Execute the Air Force Industrial Security Program consistent with the standards of DoDI 5220.22 and Federal Acquisition Regulation part 4 subpart 4.4 to assure the protection of classified information and Controlled Unclassified Information released to contractors. Procedures will require review of contract actions before award to decide if releasing classified information is necessary, and if so, will include the proper "security requirements" clauses in contracts, ensure proper security guidance to contractors, and address other relevant requirements of the industrial security program.

2.8. Execute the Air Force Personnel Security Program and policies to implement DoDI 5200.02 and assure standards and procedures for determining whether an individual's

employment, retention, and access to information are consistent with national security interests.

2.9. Ensure the development and implementation of security awareness, training, and education within all security programs.

2.10. Ensure all Airmen and others supporting the Air Force mission (military, civilian, and contractor) execute security as a personal responsibility while promoting proactive and informed execution of security requirements within the AF and its functional portfolios.

2.11. Ensure Original Classification Authority (as defined in DoD Manual 5200.01 Volume 1, *DoD Information Security Program: Overview, Classification, and Declassification*) is kept to the minimum necessary to accomplish the mission. Original Classification Authority is classification authority specific to a level of classification (Top Secret, Secret, and Confidential). Original Classification Authorities are delegated based on position.

2.11.1. Only the Secretary of the Air Force may delegate Top Secret Original Classification Authority in the Air Force. SAF/AA is hereby delegated Top Secret Original Classification Authority.

2.11.2. Only the Secretary of the Air Force and SAF/AA may delegate Secret and Confidential Original Classification Authority.

2.11.3. All original classification authorities must complete initial training upon assuming the position, prior to making any original classification authority decisions, and then annually thereafter.

2.12. Use the Air Force Security Enterprise risk management system of record to assess and manage security risk.

3. Roles and Responsibilities.

3.1. **The Air Force Security Enterprise Executive Board (AFSEEB).** The AFSEEB is the senior-level, primary governance body for management, strategic administration, and policy coordination of the Air Force Security Enterprise. The AFSEEB meets as needed, no less than annually, to address security risks and security concerns within the protection programs and security-related functions that affect daily Air Force operations and missions. The AFSEEB will:

3.1.1. Serve as the advisory council to the Secretary and Chief of Staff of the Air Force on security aspects of cross-cutting issues (e.g., critical technology protection, insider threat) involving multiple stakeholders and process owners. Additionally, the AFSEEB provides recommendations to the AF Board and AF Council on key decisions for the security enterprise to include all functional portfolios.

3.1.2. Ensure Air Force security policies are aligned with DoD security issuances.

3.1.3. Promote a proactive security environment with a philosophy that security is everyone’s responsibility.

3.1.4. Implement standardized security processes across the enterprise to the maximum extent possible and with appropriate provision for unique missions and security environments to ensure:

3.1.4.1. Maximum interoperability;

3.1.4.2. Consistent quality assurance; and

3.1.4.3. Cost savings.

3.1.5. Designate qualified personnel for sub-groups to support the AFSEEB and Defense Security Enterprise Executive Committee, when required.

3.1.6. Monitor the Air Force Security Enterprise risk management system of record and use it to inform strategy, planning, programming, budgeting and execution for the Air Force Security Enterprise.

3.2. **Administrative Assistant to the Secretary of the Air Force (SAF/AA) will:**

3.2.1. Serve as the Security Program Executive for the Air Force and represent the Air Force Security Enterprise at the Defense Security Enterprise Executive Committee. In accordance with DoDD 5200.43, the Security Program Executive is:

3.2.1.1. Designated responsibility for and authority to accomplish security program objectives for development, production, and sustainment to meet operational needs;

3.2.1.2. Accountable for credible cost, schedule, and performance reporting to the Defense Security Enterprise Executive Committee; and

3.2.1.3. Responsible for establishing programs to hire, train, and retain a professional security workforce.

3.2.2. Chair the AFSEEB.

3.2.3. Serve as the Air Force Senior Agency Official for the Information Security Program and has responsibilities for the requirements in Section 5.4.(d). of Executive Order 13526, *Classified National Security Information.*

3.2.4. Serve as the Air Force Senior Agency Official for directing and administering the DoD Personnel Security Program.

3.2.5. Oversee the reporting, investigation, referrals, and communication concerning serious security incidents involving classified information.

3.2.6. Serve as the Air Force Senior Official for establishing, implementing, and providing oversight of the Air Force Insider Threat Program.

3.2.7. Establish, develop, and implement the Air Force Industrial Security Program consistent with the standards of the National Industrial Security Program Operating Manual, the DoD Industrial Security Program, and Federal Acquisition Regulations to assure the protection of classified information and Controlled Unclassified Information released to contractors.

3.2.8. Identify technical requirements for developing capabilities within the Air Force Security Enterprise risk management system of record.

3.2.9. Manage the Original Classification Authority delegation memorandum and list of all Top Secret, Secret, and Confidential Original Classification Authority for the Air Force. SAF/AA will generate an Original Classification Authority delegation letter for Secretary of the Air Force validation and approval every two-years.

3.2.10. Ensure the integration of the security disciplines and the security-related efforts described in **paragraph 1**.

3.3. **Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics (SAF/AQ) will:**

3.3.1. Serve as a voting member of the AFSEEB.

3.3.2. Address Air Force system engineering interests by providing policy guidance.

3.3.3. Address and synchronize system security engineering related to weapon systems programs and mission components.

3.3.4. Address and synchronize a comprehensive Air Force supply chain risk management program.

3.3.5. Identify technical requirements for developing capabilities within the Air Force Security Enterprise risk management system of record.

3.3.6. Address any other security interests across the SAF/AQ functional portfolio related to the Air Force Security Enterprise or any other protection program that informs or aligns with the Air Force Security Enterprise.

3.3.7. In consultation with SAF/AA, establish contracting procedures for ensuring compliance with industrial security requirements. In particular, procedures will require review of contract actions before an award to decide if releasing classified information is necessary, and if so, will include the proper clauses in contracts, ensure proper security guidance to contractors, and address other relevant requirements of the industrial security program.

3.4. **Deputy Chief Information Officer (SAF/CN) will:**

3.4.1. Serve as a voting member of the AFSEEB.

3.4.2. Address security interests across the SAF/CN functional portfolio related to the Air Force Security Enterprise or any other protection program that informs or aligns with the Air Force Security Enterprise.

3.4.3. Address security issues related to the Enterprise Information Environment Mission Area.

3.4.4. Identify technical requirements for developing capabilities within the Air Force Security Enterprise risk management system of record.

3.5. **General Counsel of the Air Force (SAF/GC) will:**

3.5.1. In coordination with AF/JA, provide legal counsel for security enterprise functions, activities and decisions. Coordination with AF/JA will be consistent with classification or caveat restrictions.

3.5.2. In coordination with AF/JA, provide advice and counsel regarding laws and Air Force and DoD policies and regulations that are applicable to the Insider Threat Program and those pertaining to civil liberties, privacy, and whistleblower protection.

3.6. **The Inspector General of the Air Force (SAF/IG) will:**

3.6.1. Serve as a voting member of the AFSEEB.

3.6.2. Address security interests across the SAF/IG functional portfolio related to the Air Force Security Enterprise or any other protection program that informs or aligns with the Air Force Security Enterprise.

3.6.3. Oversee the Air Force Office of Special Investigations as the Air Force's sole agency for conducting counterintelligence activities; the lead agency for investigating technology transfer violations within investigative jurisdiction; and the lead agency for investigating suspected crimes targeting computer systems within its investigative jurisdiction.

3.6.4. Ensure procedures are established to securely share relevant law enforcement, counterintelligence, other analytic products, and applicable information with authorized insider threat program personnel to identify, analyze and resolve insider threat issues. Ensure those procedures are consistent with privacy laws, civil liberties, regulations, and do not jeopardize active investigations.

3.7. **Deputy Under Secretary of the Air Force, Management and Deputy Chief Management Officer (SAF/MG) will:**

3.7.1. Serve as a voting member on the AFSEEB.

3.7.2. Address security interests across the SAF/MG functional portfolio related to the Air Force Security Enterprise or any other protection program that informs or aligns with the Air Force Security Enterprise specifically as they relate to performance goals and measures for improving and evaluating the overall economy, efficiency, and effectiveness.

3.8. **Assistant Secretary of the Air Force for Manpower and Reserve Affairs (SAF/MR) will:**

3.8.1. Inform on suitability and fitness policies for Appropriated Fund (APF) and Non Appropriated Fund (NAF) civilians for employment and Common Access Card credentialing.

3.8.2. Address policy for fitness determinations for volunteers and military personnel with regular and recurring access with children, performing duties as Sexual Assault Response Coordinators or Sexual Assault Prevention and Response Victim Advocates.

3.9. **Deputy Chief of Staff, Manpower, Personnel and Services (AF/A1) will:**

3.9.1. Serve as a voting member of the AFSEEB.

3.9.2. Address security interests across the AF/A1 functional portfolio related to security workforce certification, training and position identification in appropriate databases, and the Insider Threat Program.

3.9.3. Address policy and guidance for integrating and vetting emerging institutional education and training requirements or learning outcomes into accessions, Professional Military Education, Professional Continuing Education, and ancillary training.

3.9.4. Address personnel policy and essential procedural guidance for the management of the Common Access Card credentialing for civilians and military.

3.9.5. Securely provide insider threat program personnel regular, timely, and if possible, electronic access to the information necessary to identify, analyze, and resolve insider threat matters. Such access and information include but are not limited to relevant Human Resource databases and files to include but not limited to personnel files, payroll and voucher files, outsider activities requests, disciplinary files, and personal contact records, as may be necessary for resolving or clarifying insider threat matters.

3.9.5.1. Ensure procedures are consistent with all applicable privacy laws, civil liberties, regulations and other statutes.

3.9.6. Ensure policies and procedures are established for insider threat-related information sharing in already existing violence prevention programs in accordance with all applicable privacy laws, civil liberties, regulations, and other statutes.

3.10. **Deputy Chief of Staff, Intelligence, Surveillance, Reconnaissance, and Cyber Effects Operations (AF/A2/6) will:**

3.10.1. Serve as a voting member of the AFSEEB.

3.10.2. Serve as the Air Force Head of the Intelligence Community Element and the authority for all actions regarding the security, use, and dissemination of sensitive compartmented information.

3.10.3. Make resource recommendations for the Insider Threat Program and coordinate those requirements with SAF/AA for implementation.

3.10.4. Identify technical requirements for the development of capabilities within the Air Force Security Enterprise risk management system of record.

3.10.5. Address security interests across the AF/A2/6 functional portfolio related to the Air Force Security Enterprise or any other protection program that informs or aligns with the Air Force Security Enterprise.

3.10.6. In accordance with applicable laws and policies, provide insider threat program personnel access to intelligence reporting and analytic products relevant to insider threat.

3.11. **Deputy Chief of Staff, Operations (AF/A3) will:**

3.11.1. Serve as a voting member of the AFSEEB.

3.11.2. Address security interests across the AF/A3 functional portfolio related to the Air Force Security Enterprise or any other protection programs that inform or align with the Air Force Security Enterprise.

3.11.3. Synchronize security enterprise and mission assurance efforts with the Warfighting Mission Area.

3.11.4. Identify technical requirements for developing capabilities of the Air Force Security Enterprise risk management system of record.

3.12. **Deputy Chief of Staff, Logistics, Engineering and Force Protection (AF/A4) will** :

3.12.1. Serve as a voting member of the AFSEEB.

3.12.2. Address security interests across the AF/A4 functional portfolio related to the Air Force Security Enterprise or any other protection program that informs or aligns with the Air Force Security Enterprise.

3.12.3. Identify technical requirements for developing capabilities within the Air Force Security Enterprise risk management system of record.

3.12.4. Ensure procedures are established to securely share law enforcement and other applicable information consistent with privacy laws, civil liberties and regulations with authorized insider threat program personnel to identify, analyze and resolve insider threat issues.

3.13. **Deputy Chief of Staff, Strategic Deterrence and Nuclear Integration (AF/A10) will** :

3.13.1. Serve as a voting member of the AFSEEB.

3.13.2. Serve as the Air Force OPR for Unclassified Controlled Nuclear Information (UCNI) in coordination with AF/A4.

3.13.3. Address security interests across the AF/A10 functional portfolio related to the Air Force Security Enterprise or any mission areas that inform or align with the Air Force Security Enterprise.

3.14. **The Air Force Judge Advocate General (AF/JA) will:**

3.14.1. In coordination with SAF/GC, provide legal counsel for security enterprise functions, activities and decisions and support the AFSEEB as a technical advisor.

3.14.2. In coordination with SAF/GC, provide advice and counsel regarding laws and DoD and AF policies and regulations that are applicable to the Insider Threat Program and those pertaining to civil liberties, privacy, and whistle blower protection.

3.15. **The Air Force Surgeon General (AF/SG) will:** support the AFSEEB as a technical advisor to address security equities across the AF/SG functional portfolio related to protected health information and Force Health Protection.

3.16. **Major Commands (MAJCOMs), Direct Reporting Units (DRUs), and Field Operating Agencies (FOAs) Commanders will:**

3.16.1. Ensure all Airmen and others supporting the Air Force mission (military, civilian, and contractor) execute security as a personal responsibility.

3.16.2. Ensure the proper implementation of security is directed by commanders and other leaders at every level and is fostered through awareness, education and training, and leadership.

3.16.3. Appoint a command Security Program Executive, usually the Deputy Commander, to communicate and coordinate on security issues relative to their command.

3.16.4. Integrate the various security functions to ensure an effective program.

3.16.5. Establish, develop, coordinate and implement security enterprise activities, policies and procedures for the oversight, execution, management, risk management, and administration of the command's security enterprise.

3.16.6. Report command security enterprise issues to the AFSEEB Executive Secretariat.

3.17. **The following organizations are technical advisors to the AFSEEB and will attend when requested:**

3.17.1. Auditor General of the Air Force (SAF/AG).

3.17.2. Assistant Secretary of the Air Force for Financial Management and Comptroller (SAF/FM).

3.17.3. General Counsel of the Air Force (SAF/GC).

3.17.4. Deputy Under Secretary of the Air Force for International Affairs (SAF/IA).

3.17.5. Assistant Secretary of the Air Force for Installations, Environment, and Energy (SAF/IE).

3.17.6. Assistant Secretary of the Air Force Manpower and Reserve Affairs (SAF/MR).

3.17.7. Director, Public Affairs (SAF/PA).

3.17.8. Deputy Chief of Staff, Strategy, Integration and Requirements (AF/A5).

3.17.9. Deputy Chief of Staff, Plans and Programs (AF/A8).

3.17.10. Director, Studies, Analyses and Assessments (AF/A9).

3.17.11. Air Force Surgeon General (AF/SG).

3.17.12. Air Force Judge Advocate General (AF/JA).

3.17.13. Chief of Air Force Reserve (AF/RE).

3.17.14. Director, Air Force Test and Evaluation (AF/TE).

3.17.15. Director, Air National Guard (DANG).

MATTHEW P. DONOVAN
Acting Secretary of the Air Force

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

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

Presidential Memorandum -- *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, 21 November 2012

Federal Acquisition Regulation, current edition

Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms,* April 2018, as amended

DoD Directive 5210.50, *Management of Serious Security Incidents Involving Classified Information*, 27 October 2014

DoD Directive 5200.43, *Management of the Defense Security Enterprise*, 1 October 2012

DoD Directive 5205.16, *The DoD Insider Threat Program,* 30 September 2014

DoD Instruction 5220.22, *National Industrial Security Program (NISP),* 18 March 2011

DoD Instruction 5200.01, *DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI),* 21 April 2016

DoD Instruction 5200.02, *DoD Personnel Security Program (PSP)*, 21 March 2014

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

AF Instruction 16-1402, *Insider Threat Program Management*, 5 August 2014

Air Force Manual 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

AFPD—Air Force Policy Directive

AFSEEB—Air Force Security Enterprise Executive Board

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

HAF—Headquarters Air Force

SAF—Secretariat of the Air Force

Terms

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.

Functional Portfolio—In relation to security enterprise and mission assurance, a grouping of security and mission assurance initiatives and/or programs, by capability, to accomplish a specific functional goal, objective, or mission outcome.

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.

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. With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security. (Joint Publication 1-02)