BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE POLICY DIRECTIVE 16-14

24 JULY 2014

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
(Patricia Zarodkiewicz)

Pages: 13

Supersedes: AFPD 31-4, 1 Sep 1998;
AFPD 31-5, 1 Aug 1995;
AFPD 31-6,1 Apr 2000

This directive establishes Air Force policy and responsibilities for the oversight, management and execution of the Air Force Security Enterprise. This policy directive implements Executive Order (E.O.) 13526, *Classified National Security Information*; E.O. 13556, *Controlled Unclassified Information*; E.O. 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*; E.O. 12968, *Access to Classified Information*; and Presidential Memorandum -- *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, November 2012. It provides the foundational Air Force policy for the implementation of DoD Directive (DoDD) 5200.43, *Management of the Defense Security Enterprise*; DoD 5200.2-R, *Personnel Security Program*; DoD Instruction (DoDI) 5200.02, *DoD Personnel Security Program (PSP)*; DoD *Insider Threat Program Policies*; DoDI 5200.01, *DoD Information Security Program and Protection of Sensitive Compartmented Information*; and DoDI 5220.22, *National Industrial Security Program (NISP)*. Furthermore, this policy directive aligns the DoD Security Enterprise Strategy, 2013 to the DoD Mission Assurance Strategy, 2012 under the oversight and governance of the Air Force Security Enterprise Executive Board (AFSEEB). Compliance is mandatory for all military and civilian personnel, members of the Air Force Reserve and Air National Guard, contractors and consultants (when contract performance supports the functions listed in this policy directive), and non-DoD U.S. Government Agencies whose personnel, by mutual agreement, require support from or conduct operational activity with the Air Force. This publication may not be supplemented without approval from SAF/AAZ. Refer recommended

changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Form 847 from the field through functional chain of command. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with the AF Records Disposition Schedule (RDS) maintained in the Air Force Records Information Management System (AFRIMS).

SUMMARY OF CHANGES

Incorporates the Air Force Insider Threat Program and Information Protection Programs, i.e., Information Security, Personnel Security, and Industrial Security under the cognizant authority of the Administrative Assistant to the Secretary of the Air Force. Supersedes Air Force Policy Directive (AFPD) 31-4, *Information Security Program Management*, AFPD 31-5, *Personnel Security Program*, and AFPD 31-6, *Industrial Security Program*.

1. Overview. This Policy Directive:

1.1. Establishes policy and assigns responsibilities for the management of the Air Force Security Enterprise (AFSE) as defined herein.

1.2. Establishes the Air Force Security Enterprise Executive Board (AFSEEB) as a 3-Star General Officer (GO)/ Senior Executive Service (SES) equivalent forum to provide security enterprise governance for the strategic administration, risk management, and policy coordination of the AFSE. The AFSEEB functions and membership are described in Attachment 2 of this policy directive.

1.3. Appoints the Air Force Senior Agency Official (SAO) for Security and the Security Program Executive (SPE).

2. Policy. The Air Force will:

2.1. Develop and sustain an enterprise security framework and strategic plan, incorporating mission assurance, to provide an integrated risk-managed structure to guide AFSE policy implementation, inform investment decisions, and to provide a sound basis for oversight and evolution. The AFSE is aligned with or informed by all AF security-related functions and activities.

2.2. 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.

2.3. 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 AFSE.

2.4. Use the AFSEEB to provide an enterprise-wide, integrated organizational perspective to the security enterprise and mission assurance policy development, risk management, resource advocacy, oversight, implementation and training.

2.5. Establish, develop, and implement comprehensive insider threat detection and prevention program, in accordance with E.O. 13587 and the National Insider Threat Policy

and Minimum Standards for Executive Branch Insider Threat Programs issued pursuant to E.O. 13587, and applicable DoD Insider Threat policies and guidance.

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

2.7. Establish, develop, and execute the Information Security (INFOSEC) program consistent with the DoD INFOSEC Program and applicable policies. The INFOSEC program will assure the protection of collateral classified, Sensitive Compartmented Information (SCI), Special Access Program (SAP) Information and Controlled Unclassified Information (CUI).

2.8. Establish, develop, and execute the Industrial Security program consistent with the standards of the National Industrial Security Program Operating Manual (NISPOM), the DoD Industrial Security Program, and Federal Acquisition Regulations (FAR) to assure the protection of classified information under the control of U.S. industry.

2.9. Ensure commanders at all levels and AF personnel identify and protect classified information and CUI as required by national policies to include the protection of national security classified information and CUI released to contractors.

2.10. Establish, develop, and execute the Personnel Security program and policies to implement the DoD Personnel Security Program and assure standards and procedures for determining whether an individual's employment, retention, and access to information are clearly consistent with national security interests.

2.11. Ensure the development and implementation of security awareness, training, and education programs throughout the security enterprise are executed within all security programs.

2.12. Confirm all personnel understand their security roles and responsibilities based upon the premise that security is everyone's responsibility on a day-to-day basis while promoting proactive and informed execution of security requirements within the AF and its functional portfolios.

2.13. Establish, develop, and execute an Installation Access Control program and policies to implement the DoD DTM 09-012, *Interim Policy Guidance for DoD Physical Access Control*, and assure standards and procedures for determining whether an individual's access is clearly consistent with national security interests.

2.14. Ensure Intelligence threat fusion process is properly addressed within the AFSE to provide oversight and integration of threat into the risk management picture.

3. Responsibilities.

3.1. Administrative Assistant to the Secretary of the Air Force and Air Force Senior Security Official (SAF/AA) will:

3.1.1. Serve as the Air Force Senior Agency Official (EO 13526) and Security Program Executive (DoDD 5200.43) with oversight responsibility for the Air Force Security Enterprise.

3.1.2. Represent the Air Force at the Defense Security Enterprise Executive Committee and ensure Air Force compliance with the Defense Security Enterprise strategies, policies, and procedures.

3.1.3. Provide executive oversight and program management for the Information Security, Industrial Security, Personnel Security, Nuclear Information Security, and Air Force Insider Threat programs.

3.1.4. Serve as the Chair for the AFSEEB and appoint an executive secretariat to provide administrative support.

3.1.5. Appoint a GO/SES equivalent within SAF/AAZ as a member of the AFSEEB to address security equities across the SAF/AA functional portfolio related to Personnel Security, Information Security, Industrial Security, Special Access Program policy; Nuclear Information Security; and the Insider Threat Program.

3.1.6. Coordinate career field specific education and training requirements with the respective career field managers for integration into Career Field Education and Training Plan (CFETP)/Specialty Training Standard (STS)/Course Training Standard (CTS) as appropriate.

3.2. Auditor General of the Air Force (SAF/AG) will support the AFSEEB as a technical advisor to address security equities related to internal security enterprise and mission assurance audits.

3.3. Assistant Secretary of the Air Force for Acquisition (SAF/AQ) will serve as a member of the AFSEEB as the subject matter expert on security matters for acquisition programs throughout the life cycle (materiel development decision to demilitarization).

3.4. Chief of Information Dominance and Chief Information Officer (SAF/CIO A6) will:

3.4.1. Serve as a member of the AFSEEB to address security equities across their functional portfolio related to cybersecurity (formerly Information Assurance), information technology, cyber security, privacy program, insider threat, and cyber security initiatives related to the defense industrial base.

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

3.5. Assistant Secretary of the Air Force Financial Management and Comptroller (SAF/FM) will support the AFSEEB as a technical advisor to address security equities related to security enterprise costs and economics.

3.6. General Counsel of the Air Force (SAF/GC) will support the AFSEEB as a technical advisor and provide legal counsel for security enterprise and mission assurance functions, activities and decisions.

3.7. Deputy Undersecretary of the Air Force for International Affairs (SAF/IA) will support the AFSEEB as a technical advisor to address security equities across their functional portfolio related to foreign disclosure; security cooperation; and export control.

3.8. Assistant Secretary of the Air Force Installations, Environment and Logistics (SAF/IE) will support the AFSEEB as a technical advisor to address security equities across their functional portfolio related to energy security.

3.9. Inspector General (SAF/IG) will serve as a member of the AFSEEB to address security equities across their functional portfolio related to security compliance inspection policy; criminal investigations; counterintelligence oversight and operations; complaints; fraud, waste and abuse; and insider threat programs.

3.10. Assistant Secretary of the Air Force Manpower & Reserve Affairs (SAF/MR) will support the AFSEEB as a technical advisor to address security equities across their functional portfolio related policy oversight of human resources and Air Reserve component programs.

3.11. Director, Public Affairs (SAF/PA) will support the AFSEEB as a technical advisor and perform security and policy reviews for the clearance of information, imagery and video proposed for public release.

3.12. Director Business Transformation, Deputy Chief Management Officer (SAF/US (M)) will:

3.12.1. Serve as a member of the AFSEEB to address security equities across their functional portfolio related to performance goals and measures for improving and evaluating overall economy, efficiency, and effectiveness of the security enterprise.

3.12.2. Address security issues related to the Business Mission Area (BMA).

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

3.13.1. Serve as a member of the AFSEEB to address security equities across their functional portfolio related to security workforce certification, training and position identification in appropriate databases, and the insider threat program.

3.13.2. Provide policy and guidance for integrating and vetting new/emerging institutional education and training requirements or learning outcomes into accessions, Professional Military Education (PME), Professional Continuing Education (PCE) and ancillary training.

3.14. Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance (AF/A2) will:

3.14.1. Serve as a member of the AFSEEB to address security equities across their functional portfolio related to intelligence oversight, sensitive compartmented information, threat analysis and reporting, and the insider threat program.

3.14.2. Address security issues related to the Defense portion of the Intelligence Mission Area.

3.15. Deputy Chief of Staff, Operations, Plans and Requirements (AF/A3/5) will:

3.15.1. Serve as a member of the AFSEEB to address security equities across their functional portfolio related to operations security, cyber security, defense critical infrastructure, continuity of operations, chemical, biological, radiological and nuclear survivability, counter threat development, and the insider threat program.

3.15.2. Address and synchronize security enterprise and mission assurance efforts with the Warfighting Mission Area.

3.16. Deputy Chief of Staff, Logistics, Installations and Mission Support (AF/A4/7) will serve as a member of the AFSEEB to address security equities across their functional portfolio related to: mission assurance to include integrated defense; antiterrorism; physical

security; law enforcement; installation emergency management; fire emergency services; explosive ordnance disposal; chemical, biological, radiological and nuclear (CBRN) consequence; force protection; management/passive defense; nuclear physical security; and the insider threat program.

3.17. Deputy Chief of Staff, Strategic Plans and Programs (AF/A8) will support the AFSEEB as a technical advisor to address security equities across their functional portfolio related to strategic planning and programming of Air Force security portfolio and capabilities.

3.18. Director, Analyses, Assessments and Lessons Learned (AF/A9) will support the AFSEEB as a technical advisor to address security equities across their functional portfolio related to timely analyses, assessments, and lessons learned supporting the Air Force security portfolio and capabilities.

3.19. Assistant Chief of Staff, Strategic Deterrence & Nuclear Integration (AF/A10) will serve as a member of the AFSEEB to address security equities across their functional portfolio related to the nuclear enterprise.

3.20. The Judge Advocate General (AF/JA) will in coordination with the General Counsel, support the AFSEEB as a technical advisor and provide legal counsel for security enterprise and mission assurance functions, activities and decisions.

3.21. Air Force Surgeon General (AF/SG) will support the AFSEEB as a technical advisor to address security equities across their functional portfolio related to protected health information (PHI) and Force Health Protection; and the insider threat program.

3.22. Chief of Air Force Reserve Affairs (AF/RE) will support the AFSEEB as a technical advisor to address security equities across their functional portfolio related to Reserve affairs.

3.23. Director, Air Force Test and Evaluation (AF/TE) will support the AFSEEB as a technical advisor to address security equities across their functional portfolio related to credible test and evaluation in all phases of the system's life cycle and the security enterprise.

3.24. Director, Air National Guard (NGB/CF) will support the AFSEEB as a technical advisor to address security equities across their functional portfolio related to Air Guard affairs.

3.25. Major Commands (MAJCOMs) and Direct Reporting Units (DRUs) Commanders will:

3.25.1. Appoint a MAJCOM SPE to communicate and coordinate on security issues relative to their command and implement a standardized command security structure to support an enterprise framework.

3.25.2. Integrate the various security functions into a standardized structure to ensure consistence compliance is leveraged through standardized guidelines, inspections, regulations and other measures.

3.25.3. Establish, develop, coordinate and implement security enterprise activities, policies and procedures for the oversight, execution, management, risk management, and administration of the MAJCOM/DRU security enterprise.

3.25.4. Report security enterprise issues through their HAF functional leads, the Security Enterprise - Mission Assurance Steering Group, and when appropriate, to the AFSEEB through the AFSEEB Executive Secretariat.

3.25.5. Ensure proper maintenance of records for the MAJCOM Security Enterprise.

3.26. Core Function Leads will address equities in their respective areas of responsibility through their HAF functional leads.

DEBORAH LEE JAMES
Secretary of the Air Force

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

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

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

Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, 7 October 2011

Executive Order 12968, *Access to Classified Information*

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

Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, as Amended 15 March 2014

National Industrial Security Program Directive No. 1, Volume 75, Number 65, 6 April 2010

DoDD 5100.55, United States Security Authority for North Atlantic Treaty Organization Affairs (USSAN), 27 February 2006

DoDD 5210.50, Unauthorized Disclosure of Classified Information to the Public, 22 July 2005

DoDD 5230.11, Disclosure of Classified Military Information to Foreign Governments and International Organizations, 16 June 1992

DoDD 5230.20, Visits and Assignments of Foreign Nationals, 22 June 2005

DoDD 5200.43, *Management of the Department of Defense Security Enterprise*, 1 October 2012

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

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

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

DoD DTM 09-12, *Interim Policy Guidance for DoD Physical Access Control*, 22 April 2014

Defense Security Enterprise Strategic Plan, May 2013

DoD Mission Assurance Strategy, April 2012

DoD Mission Assurance Framework, October 2013

Air Force Instruction 90-802, *Risk Management*, 11 February 2013

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AFPD—Air Force Policy Directive

AFSE—Air Force Security Enterprise

AFSEEB—Air Force Security Enterprise Executive Board

COOP—Continuity of Operations

CUI—Controlled Unclassified Information

HAF—Headquarters Air Force

IA—Information Assurance

IC—Intelligence Community

MA—Mission Assurance

SEMASG—Security Enterprise and Mission Assurance Steering Group

OPR—Office of Primary Responsibility

PA—Public Affairs

SAP—Special Access Program

SCI—Sensitive Compartmented Information

SPE—Security Program Executive

Terms

Air Force Security Enterprise— The organizations, infrastructure, and measures (to include policies, processes, procedures, and products) in place to safeguard AF personnel, information, operations, resources, technologies, facilities, and assets against harm, loss, or hostile acts and influences. The AFSE 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 (CBRN) consequence management and passive defense; energy and critical infrastructure security; special access program security policy; critical program information protection policy; security planning and policy for acquisition life cycle management; antiterrorism; insider threat; and security training. AFSE aligns with counterintelligence, intelligence, information assurance, 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 policy.

Controlled Unclassified Information— A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification but is pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government and under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. The designation CUI replaces the term "sensitive but unclassified" (SBU).

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.

Governance— The Air Force's ability to serve its members through the rules, processes, and behavior by which interests are articulated, resources are managed, and power is exercised to

accomplish its statutory responsibilities. The key to effective governance at any staff level is a representative participatory decision-making process.

Industrial Security— Those policies, practices and procedures that ensure maximum uniformity and effectiveness safeguarding classified and sensitive information in the possession and control of U.S. industrial organizations, educational institutions, and all organizations and facilities used by prime and subcontractors"

Information Security— Those policies, practices and procedures that ensure the proper marking, protection, and dissemination of controlled unclassified information (CUI) and classified information, including information categorized as collateral, sensitive compartmented information (SCI), and Special Access Program (SAP)."

Insider Threat— The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

Insider Threat Program— The area of the security enterprise that is concerned with the policies, procedures, and activities to prevent and mitigate acts of harm by authorized personnel to the security of the Air Force and the United States.

Integration— In relation to the AFSE, the identification of risks and interdependencies between functions and processes within the enterprise and the development of managed process solutions to address those risks and interdependencies. It is not integration, but rather it is about integrating the protection disciplines with the mission to deliver value. It relies on a common view of mission across the disparate risk domains and a common framework from which to operate. The converged approach reaches across people, processes, and technology and enables the enterprise to prevent (as it pertains solely to intentional/hostile threats), detect, respond to, and recover from any type of incident.

Mission Assurance— A process to protect or ensure the continued function and resilience of capabilities and assets – including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains – critical to the performance of DoD Mission Essential Functions (MEF) in any operating environment or condition.

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

Personnel Security— Those policies, practices and procedures to ensure that acceptance and retention of personnel in the Armed Forces, acceptance and retention of civilian employees in the Department of Defense, and granting 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.

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

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

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. (JP 1-02). AFSE defines as proactive measures adopted to safeguard personnel, information, operations, resources, technologies, facilities, and foreign relations against harm, loss, or hostile acts and influences.

Security Program Executive—The designated individual with responsibility for and authority to accomplish security program objectives for development, production, and sustainment to meet operational needs. The security program executive shall be accountable for credible cost, schedule, and performance reporting to the Defense Security Executive.

Attachment 2

AIR FORCE SECURITY ENTERPRISE EXECUTIVE BOARD (AFSEEB)

A2.1. Purpose. The AFSEEB is the senior-level governance body for the strategic oversight, administration, policy synchronization, resource review and prioritization, and risk management activities of the AFSE. In that role, it shall:

A2.1.1. Advise the Secretary of the Air Force and Chief of Staff Air Force on security and mission assurance matters. Additionally, the AFSEEB provides recommendations to the AF Board and AF Council on key decisions for the security enterprise to include all functional portfolios.

A2.1.2. Develop a security framework to integrate all security functions to support information sharing, collaboration on cross-functional security issues, resource requirements, and risk mitigation activities.

A2.1.3. Ensure the development, advocacy, and defense of the AFSE in support of the Defense Security Enterprise Executive Committee (DSE EXCOM).

A2.1.4. Commission reviews and in-depth studies of security issues and, based on results, make recommendations for developing or improving policies, processes, procedures, and products to address pervasive, enduring, or emerging security challenges.

A2.1.5. Identify performance and reporting measures to be used to assess the effectiveness of the AFSE program and its contribution to mission success.

A2.2. Membership. The AFSEEB members will ensure security issues within their functional portfolios are vetted through the AFSEEB. The AFSEEB voting members consist of:

A2.2.1. Air Force Security Program Executive will serve as the Chair (SAF/AA).

A2.2.2. Director, Security and Special Program Oversight (SAF/AAZ)

A2.2.3. Assistant Secretary of the Air Force for Acquisition (SAF/AQ)

A2.2.4. Chief of Information Dominance and Chief Information Officer (SAF/CIO A6)

A2.2.5. Air Force Inspector General (SAF/IG)

A2.2.6. Director, Business Transformation, Deputy Chief Management Officer (SAF/US(M))

A2.2.7. Deputy Chief of Staff, Manpower, Personnel and Services (AF/A1)

A2.2.8. Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance (AF/A2)

A2.2.9. Deputy Chief of Staff, Operations, Plans and Requirements (AF/A3/5)

A2.2.10. Deputy Chief of Staff, Logistics, Installations and Mission Support (AF/A4/7)

A2.2.11. Assistant Chief of Staff, Strategic Deterrence & Nuclear Integration (AF/A10)

A2.3. Technical Advisors. The AFSEEB technical advisors meeting attendance is based on meeting agenda or the direction of the AFSEEB Chair. The technical advisors consist of:

A2.3.1. Auditor General of the Air Force (SAF/AG)

A2.3.2. Assistant Secretary of the Air Force Financial Management and Comptroller (SAF/FM)

A2.3.3. General Counsel of the Air Force (SAF/GC)

A2.3.4. Deputy Undersecretary of the Air Force for International Affairs (SAF/IA)

A2.3.5. Assistant Secretary of the Air Force Installations, Environment, and Logistics (SAF/IE)

A2.3.6. Assistant Secretary of the Air Force Manpower & Reserve Affairs (SAF/MR)

A2.3.7. Director, Public Affairs (SAF/PA)

A2.3.8. Deputy Chief of Staff, Strategic Plans and Programs (AF/A8)

A2.3.9. Director, Analyses, Assessments, and Lessons Learned (AF/A9)

A2.3.10. Air Force Surgeon General (AF/SG)

A2.3.11. Air Force Judge Advocate General (AF/JA)

A2.3.12. Chief of Air Force Reserve Affairs (AF/RE)

A2.3.13. Director, Air Force Test and Evaluation (AF/TE)

A2.3.14. Director, Air National Guard (NGB/CF)

A2.4. Meetings. The AFSEEB shall meet no less than semiannually and as required at the discretion of the Chair. The Chair shall set the agenda with input from the members. Attendance is limited to the Principal or Deputy. Any variance must be approved by the AFSEEB Chair.

A2.4.1. the AFSEEB meetings are decisional. Content of the meetings will address health of the security enterprise, security performance metrics, mission assurance equities, risk management activities, resource recommendations, and address emerging threats.

A2.4.2. Meeting minutes, to include action items, will be recorded and tracked by the AFSEEB Secretariat.

A2.5. Steering Group. The AFSEEB will be supported by the Security Enterprise and Mission Assurance Steering Group, (a three letter GO/SES level body) and the Security Enterprise and Mission Assurance Working Group (an O-6/GS-15 level body). Both steering group and working group will operate with Chair and Vice Chair from SAF/AAZ and AF/A7S respectively. The Security Enterprise and Mission Assurance Working Group is the entry point for security enterprise and mission assurance issues into the AFSE governance structure. The Security Enterprise Steering Group will make recommendations to the AFSEEB and serve as the decision point for what issues go forward to the AFSEEB. Subordinate standing or ad hoc working groups will be formed and disbanded at the direction of the Steering and Working Groups Chair / Vice Chair or as required.