BY ORDER OF THE SECRETARY OF THE AIR FORCE

DEPARTMENT OF THE AIR FORCE POLICY DIRECTIVE 16-14

29 JULY 2025

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/OCS — Certified by: SAF/OC

Supersedes: AFPD16-14, 31 December 2019 — Pages: 25

This publication implements Department of Defense (DoD) Directive (DoDD) 5200.43, *Management of the Defense Security Enterprise*; DoDD 5205.07, *Special Access Program (SAP) Policy*; DoDD 5210.50, *Management of Serious Security Incidents Involving Classified Information*; DoDI 5205.16, *The DoD Insider Threat Program*; National Security Presidential Memorandum 28, *The National Operations Security 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)*; DoDI 5200.48, *Controlled Unclassified Information (CUI)*; DoDI 5220.31, *National Industrial Security Program (NISP)*; and DoDI 5205.85, *Enhanced Security Program to Support the DoD Innovation Initiative.* This publication applies to all Department of the Air Force (DAF) civilian employees and uniformed members of the United States Space Force (USSF), Regular Air Force (RegAF), 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 publications, foreign nationals on a DAF installation obligated under an international agreement to abide by the terms of DAF publications, non-DoD U.S. government agencies whose personnel, by mutual agreement, require support from or conduct operational activity with the DAF, and personnel who require access to SAPs for which the DAF has cognizance. Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. Refer recommended changes and questions about this publication to the office of primary responsibility (OPR) listed above, using the DAF Form 847, *Recommendation*

for Change of Publication, and route DAF Forms 847 from the field through the appropriate functional chain of command. This DAF policy directive may not be supplemented.

SUMMARY OF CHANGES

This publication has been substantially revised and must be reviewed in its entirety. Major changes encompass the inclusion of the USSF, reformatting to comply with current publication guidance, removal of the Enterprise Protection Risk Management tool as a system of record, and updates roles and responsibilities within the security enterprise. Additionally, this publication incorporates and cancels security policy portions of AFPD 16-7, *Special Access Programs*, transferring and updating security roles and responsibilities from AFPD 16-7 to this publication, and leaving non-security roles from AFPD 16-7 such as planning, programming, budgeting and execution (PPB&E) to other referenced policies governing those processes.

1. Overview. The DAF Security Enterprise (DAFSE) is a mission critical function whose positions are designated as National Security positions. The enterprise provides a framework for integrating personnel security, Presidential support program vetting activities, industrial security, information security, controlled unclassified information, counter-insider threat program (C-InTP), SAP, and associated security education, training, and awareness (SETA).This framework aligns with physical security, operations security (OPSEC), counterintelligence, sensitive compartmented information (SCI), information operations, acquisition security, foreign disclosure, security cooperation, technology transfer, export control, cybersecurity, nuclear security, chemical and biological agent security, antiterrorism, force protection, mission assurance, and is informed by other security-related and enabling efforts. Implementing the DAFSE framework supports the DoD's priorities of 'reestablishing deterrence' and 'rebuilding our military'.

2. Policy. The DAF will:

2.1. Implement standardized security processes, safeguards, controls, and countermeasures to reduce risk and maximize interoperability to ensure consistent quality assurance and cost efficiencies across unique mission and operational environments.

2.2. Ensure senior leaders and functional leads collaborate on various issues potentially impacting the DAFSE such as incident response, resource allocation, risk management, policy integration, training, and other areas.

2.3. Use the DAF Security Enterprise Executive Council (DAFSEEC) and its governance structure to provide an enterprise-wide and integrated organizational perspective to support DAFSE policy development, risk management and response, resource advocacy, oversight, and training.

2.4. Execute the C-InTP consistent with the standards and requirements prescribed in DoDD 5205.16, *The DoD Insider Threat Program* while integrating with and prescribing responsibilities to the appropriate functional leads.

2.5. Execute the DAF information security program consistent with the standards in DoDI 5200.01, *DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)*. The information security program provides guidance on classification, declassification, and safeguarding of classified information.

2.6. Execute the DAF CUI program consistent with the standards in DoDI 5200.48. The CUI program provides guidance on identifying, safeguarding, disseminating, marking, storing, transmitting, reviewing, transporting, decontrolling, and destroying CUI.

2.7. Execute DAF SAP responsibilities consistent with the standards in DoDD 5205.07. SAPs under DAF cognizance will comply with all statutes, Presidential direction, applicable regulations, directives, and instructions. DAF leaders are accountable for the use of exceptions permitted in those rules or obtaining waivers from authorities responsible for those rules, as applicable. All waiver requests will be submitted to the Special Security Directorate, DAF SAP Central Office (SAF/OCS) for Secretary of the Air Force (SecAF) or Office of the Secretary of Defense (OSD) approval.

2.8. Execute the DAF industrial security program consistent with the standards of DoDI 5220.31, *National Industrial Security Program (NISP)*, Federal Acquisition Regulation (FAR), Defense Federal Acquisition Regulation Supplement (DFARS), and the Department of the Air Force Federal Acquisition Regulation Supplement (DAFFARS)to ensure the protection of classified information and CUI released to contractors. The industrial security program provides procedures for reviewing contract actions to determine if contractors require access to classified information in performance of the contract. The industrial security program 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.

2.9. Execute the DAF personnel security program consistent with standards identified in DoDI 5200.02, *DoD Personnel Security Program (PSP)*, to assure standards and procedures for national security eligibility for access determinations; personnel security actions; continuous vetting (CV); and security education requirements for employees seeking eligibility for access to classified information.

2.10. Execute DAF Presidential Support Program – Yankee White (PSP-YW) responsibilities consistent with the standards in DoDD 5210.55, *Department of Defense Presidential Support Program*, and DoDI 5210.87, *Selection of DoD Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities (PSAs)*, to ensure only the most suitable and qualified personnel are nominated, assigned, and retained for Presidential support duties.

2.11. Execute the DAF Enhanced Security Program to support the DoD Innovation Initiative and policies to implement DoDI 5205.85, *Enhanced Security Program to Support the DoD Innovation Initiative*, enabling access to innovative technologies and solutions to better leverage commercial technology.

2.12. Integrate DAF OPSEC programs with counterintelligence and other security programs, including programs used to address insider threat, CUI, data loss prevention, cybersecurity, foreign access management, physical security, industrial security, and information security, consistent with National Security Presidential Memorandum 28, *The National Operations Security Program*.

2.13. Ensure Original Classification Authority (OCA), as defined in DoD Manual (DoDM) 5200.01 Vol 1, *DoD Information Security Program: Overview, Classification, and Declassification*, is implemented appropriately. OCA is the classification authority specific to a level of classification (Top Secret, Secret, and Confidential). OCAs are delegated classification authority based on their position.

2.14. Ensure the development and implementation of SETA, within all security programs.

2.15. Ensure all DAF personnel and those with a contractual obligation to abide by the terms of DAF publications are trained on their personal responsibility to adhere to security requirements.

2.16. Synchronize and integrate Defense Security Enterprise and insider-threat policies and efforts with the Mission Assurance construct in accordance with DoDD 3020.40, *Mission Assurance.*

2.17. Integrate security policies and practices consistent with the standards in Defense Security Cooperation Agency (DSCA) Manual 5105.38-M, Security Assistance Management Manual, for DAF programs involved with government-to-government international transfers, Foreign Military Sales, cooperative research, development, acquisition, or support international agreements, and other programs designed to build Partner Nation capacity.

2.18. Integrate security into acquisition processes consistent with the standards in DoDI 5000.83, *Technology and Program Protection to Maintain Technological Advantage*, to protect weapons systems and related sensitive technology; technical information such as research data with military applications; and support systems from foreign intelligence collection, unauthorized disclosure, sabotage, theft, or damage throughout the technology's life cycle.

3. Roles and Responsibilities.

3.1. **The DAF Security Enterprise Executive Council (DAFSEEC).** The DAFSEEC is the two-letter/level 2 (2ltr/L2) governance body for the management, strategic administration, and coordination of policy, guidance, and strategy regarding the DAFSE. The DAFSEEC and principal attendees will meet as needed, no less than annually, to address security risks and concerns within information protection programs and security-related functions. The DAFSEEC will:

3.1.1. Serve as the advisory council to the Chief of Staff of the Air Force, Chief of Space Operations, Under Secretary of the Air Force (USecAF), and SecAF on security aspects of cross-cutting issues (e.g., critical technology protection, horizontal protection, insider threat, personnel vetting) involving multiple stakeholders and process owners.

3.1.2. Provide recommendations to the DAF Board and DAF Council on key decisions for the security enterprise to include all functional portfolios.

3.1.3. Ensure DAF security policies are adequately aligned to the Defense Security Enterprise (DSE) Strategy and are integrated with other publications that support the DAFSE, including counterintelligence.

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

3.1.4.1. Maximum interoperability.

3.1.4.2. Consistent quality assurance.

3.1.4.3. Cost savings.

3.1.5. Establish and identify DAFSE goals and objectives that support and enable successful implementation, execution, or sustainment of the DSE Strategy.

3.2. **The DAF Security Enterprise Executive Board (DAFSEEB).** The DAFSEEB is the three-letter/Level 3 (3ltr/L3) governance body for the management, strategic administration, and coordination of policy, guidance, and strategy regarding the DAFSE. The DAFSEEB and senior leader attendees will meet as needed, no less than bi-annually, to address security risks and concerns within the protection programs and security-related functions. The DAFSEEB will:

3.2.1. Serve as a board of senior leaders that collectively oversee and deliberate efforts regarding emerging requirements, policy, oversight, guidance, and strategy for the DAFSE.

3.2.2. Provide decisional briefings to the DAFSEEC regarding strategic administration and enterprise management of the DAFSE.

3.2.3. Advise and inform the DAFSEEC of emerging or current requirements, challenges, and issues that require principal level advocacy or authority to overcome or adequately address.

3.2.4. Designate qualified personnel to participate in sub-groups that will collaborate and inform the DAFSEEB and DAFSEEC, as needed.

3.2.5. Establish, monitor and provide oversight of sub-working groups, as needed.

3.2.6. Monitor, oversee, and support efforts to implement the DSE Strategy.

3.3. **Director, Office of Competitive Activities (SAF/OC**) will:

3.3.1. Establish and serve as the Chair of the DAFSEEC.

3.3.2. Designate the Director, SAF/OCS to establish and serve as the Chair of the DAFSEEB.

3.3.3. Serve as the DAF Security Program Executive (SPE) and represent the DAFSE at the Defense Security Enterprise Executive Committee (DSE EXCOM). In accordance with DoDD 5200.43, *Management of the Defense Security Enterprise*, the SPE will:

3.3.3.1. Ensure DAF security policies are aligned with DoD issuances.

3.3.3.2. Oversee the development, production, and sustainment of security program objectives to meet the DAF's operational needs.

3.3.3.3. Oversee accountability for providing cost share, schedule, and performance data as needed to the Defense Security Executive.

3.3.3.4. Develop and implement standardized security processes across the enterprise to maximize interoperability while applying appropriate provisions for unique missions or requirements.

3.3.3.5. Designate qualified personnel for sub-groups to support the DSE EXCOM, as required.

3.3.3.6. Promote a proactive security environment and culture that instill security awareness and personal responsibility across the DAF.

3.3.3.7. Provide data and metrics to inform decision-makers of security risk, evaluation effectiveness, and identify trends to support program improvement.

3.3.4. Serve as the DAF senior agency official, executing the following responsibilities:

3.3.4.1. Fulfill requirements identified in Section 5.4.(d). of Executive Order (E.O.) 13526, *Classified National Security Information.*

3.3.4.2. Oversee establishment, implementation, and sustainment of the DAF C-InTP.

3.3.4.3. Oversee establishment, implementation, and sustainment of the DAF personnel security program.

3.3.4.4. Oversee and conduct planning, programming, budgeting, and execution (PPBE) activities associated with the DAF personnel security investigations (PSI) budget, including analyzing and validating the classification of information across the DAF that generates PSI cost to the DAF, utilizing the DAFSEEB to develop proposals on efficiency and mission execution for DAFSEEC approval.

3.3.4.5. Oversee establishment, implementation, and sustainment of the DAF industrial security program.

3.3.4.6. Oversee establishment, implementation, and sustainment of the DAF CUI program.

3.3.4.7. Oversee establishment and implementation of the DAF information security program per DoDI 5200.01.

3.3.4.8. Oversee establishment and implementation of the DAF declassification program, and ensure necessary resources are applied to the review of information to ensure it is neither classified for longer than necessary nor declassified prematurely.

3.3.4.9. Oversee the reporting and communications concerning CUI and classified security incidents.

3.3.4.10. Oversee implementation of the DSE Strategy and ensure coordination is conducted with DAFSE stakeholders.

3.3.4.11. In consultation with SAF/AQ, establish procedures for ensuring compliance with Acquisition Security. Specifically, implement procedures for the security community's workforce to identify and develop skills necessary to support relevant Acquisition Security activities.

3.3.5. Oversee the DAF Special Access Program Central Office (SAPCO).

3.3.6. Designate the Director, Special Security Directorate (SAF/OCS) as DAF SAPCO Director. As DAF SAPCO Director, SAF/OCS will:

3.3.6.1. Ensure efficient and effective implementation of SAP policy, management, security administration, and oversight following processes similar to, but distinctly separate from, those used for non-SAP implementation.

3.3.6.2. Execute the responsibilities of SecAF, DoD Component Head with cognizant authority over SAPs, as defined in DoDD 5205.07, utilizing the governance structure outlined in **Attachment 2** of this issuance.

3.3.6.3. Oversee SAP security, audit, compliance, cybersecurity activities, and reporting requirements for assigned SAPs and SAP accredited spaces.

3.3.6.4. Appoint, in coordination with SAF/CNZ, cybersecurity representatives to DoD SAP information technology working groups.

3.3.6.5. Authorize all DAF SAP networks, databases, and information systems, including those that support SAP oversight and governance.

3.3.6.6. Appoint authorizing officials for SAP information systems and accrediting officials for SAPFs.

3.3.6.7. Ensure a dedicated cadre exists to administer and execute SAP security, audit, compliance, and cybersecurity activities for assigned SAPs, and provide oversight to these functions and personnel.

3.3.6.8. Develop and recommend HQ DAF-wide SAP inspection special emphasis items.

3.3.6.9. Implement relief of relieve DCSA security cognizance over SAP activities, also known as "carve out," in accordance with DoDI 5205.11, *Management, Administration, and Oversight of DoD Special Access Programs*.

3.3.6.10. Ensure, in coordination with SAF/CNZ, complete and thorough annual inventory of SAP information technology systems.

3.3.6.11. Implement the Undersecretary of Defense for Intelligence and Security (USD(I&S))-issued security policies and training requirements via the DoD SAP oversight bodies established in DoDD 5205.07 and DoDI 5205.11.

3.3.6.12. Coordinate, via the Director, DoD SAPCO, participation by foreign governments in joint SAPs and sharing of SAP-protected capabilities and information.

3.3.6.13. Facilitate international agreements, in coordination with SAF/IA, for foreign government involvement with DoD SAPs.

3.3.6.14. Coordinate with Director, DoD SAPCO, on SAP security matters; identifying trends; and making SAP security policy recommendations to the USD(I&S).

3.4. **Auditor General of the Air Force (SAF/AG**) has overall responsibility for the internal audit mission and is also responsible for the audit liaison and follow-up functions for DAF, to include DAFSE programs..

3.5. **Assistant Secretary of the Air Force for Acquisition, Technology and Logistics (SAF/AQ) and Assistant Secretary of the Air Force for Space Acquisition and Integration (SAF/SQ),** as the component acquisition executives, will:

3.5.1. In consultation with SAF/OC, provide guidance and oversight for acquisition security activities consistent with the standards of DoDI 5000.83 and DoDI5000.83_DAFI63-113, *Technology and Program Protection to Maintain Technological Advantage* and DAFI 63-101/20-101 *Integrated Life Cycle Management.*

3.5.2. Integrate and synchronize system security engineering, program protection support, and other related activities to develop acquisition policy and processes to support the DAFSE.

3.5.3. Address any other security interests across the SAF/AQ functional portfolio related to the DAFSE or any other protection program that informs or aligns with the DAFSE.

3.5.4. Provides the DAF recommendations for the disposition of cases under consideration by the Committee on Foreign Investment in the U.S. (CFIUS). For SAP equities, SAF/AQ and/or SAF/SQ will provide recommendations to DoD SAPCO through the DAF SAPCO for incorporation into the OSD response.

3.5.5. Implement and ensure compliance with National Industrial Security Program and for SAPs, coordinate with AFOSI PJ."

3.5.6. Informs DAF and DoD SAPCOs of SAP-related congressional engagements..

3.6. **Office of the Chief Information Officer (SAF/CN)** will:

3.6.1. Oversee the development and integration of policies, standards, and procedures for DAF information technology, cybersecurity, and mission assurance capabilities, activities, and processes, in accordance with the authorities designated to the Chief Information Officer under 44 USC 3506 and the Chief Information Security Officer under 44 USC 3544."

3.6.2. Provide guidance and facilitate actions that will enable the C-InT Hub to implement and execute user activity monitoring on classified and unclassified DAF-owned or operated networks and systems.

3.6.3. Develop and maintain a DAF SAP enterprise information technology (IT) strategy that provides information technology investment inputs to achieve desired core mission capabilities, and review and approve DAF SAP information technology acquisition consistent with the standards of Title 40 United States Code (USC) § 11101, et. Seq., *Clinger-Cohen Act of 1996,* and applicable statutes.

3.6.4. Ensure compliance with DAF policies to oversee the implementation of statutory requirements and publications for SAPs under DAF cognizance, consistent with DoD enterprise-level defense strategies from the cyberspace or IT, and national security system perspectives.

3.6.5. Ensure policy, compliance tools, and other resources developed and disseminated are coordinated with DAFSE stakeholders.

3.7. **Assistant Secretary of the Air Force (Financial Management and Comptroller) (SAF/FM)** will:

3.7.1. Oversee financial policy and management of the DAFSE financial structure.

3.7.2. Oversee fiscal accountability, cost and economic analysis, financial reporting of SAP resources, and budgeting and financial execution activities for SAPs, for which the SecAF is the cognizant authority, or in which the DAF participates with other components or agencies.

3.7.3. Notify the appropriate government activity manager (GAM) and the DoD SAPCO through DAF SAPCO of meetings with congressional committees.

3.8. **Secretary of the Air Force General Counsel (SAF/GC)** and **Air Force Judge Advocate (AF/JA)** will provide legal services to the DAFSE.

3.9. **Deputy Under Secretary of the Air Force for International Affairs (SAF/IA)** will:

3.9.1. Develop a strategy to share SAP information with coalition partners.

3.9.2. Coordinate with DAF SAPCO to gain Deputy Secretary of Defense (DEPSECDEF) approval on requests to disclose SAP information under DAF cognizance or enter into agreements with foreign entities.

3.9.3. Establish procedures for foreign disclosure within the DAFSE as reflected in AFPD 16-2, *Disclosure of Military Information to Foreign Governments and International Organizations,* and its implementing DAF publications. This will include coordination for release of SAP information as prescribed. Coordinate with AF/A2/6 and SF/S2 to ensure military and national intelligence equities and procedures are included in DoDM 5205.07, *Special Access Program Security Manual.* broader DAF disclosure processes and guidance.

3.9.4. In consultation with SAF/OC, provide guidance and oversight for international programs security activities, consistent with the standards of DAFMAN 16-101, *Security Cooperation (SC) and Security Assistance (SA) Management*.

3.10. **Department of the Air Force Inspector General (SAF/IG)** will:

3.10.1. Establish inspection policy, guidance, and oversight for DAF Inspector General (IG) functional inspections, assessments, and/or evaluations.

3.10.2. In coordination with SAF/OCS and Air Force Office of Special Investigations (AFOSI), Office of Special Projects (AFOSI PJ), conduct program security and government compliance inspections of industry, Major Command (MAJCOM), Field Command (FLDCOM), direct reporting unit (DRU), and field operating agency (FOA) SAP program offices consistent with the standards of DoD guidance and DAF policies.

3.10.3. Execute a comprehensive counterintelligence security program for all SAPs under DAF cognizance, through AFOSI PJ.

3.10.4. Establish a credibility assessment program for personnel accessed to SAPs, in accordance with DoDD 5210.48, *Credibility Assessment (CA) Program*.

3.10.5. Provide program security services for industry through AFOSI PJ, when a carve-out provision is approved by the Secretary of Defense (SECDEF) or DEPSECDEF.

3.10.6. Establish procedures for reporting fraud, waste, abuse, and corruption involving the DAFSE. A separate, secure means will be established for classified SAP reports.

3.10.7. Investigate suspected crimes within the confines of their investigative jurisdiction and authority that involve the targeting of computer systems, technology transfer violations, and other suspected nefarious activities impacting the security enterprise and security related efforts.

3.10.8. In coordination with AFOSI, ensure procedures are established with the C-InTP to allow regular, timely, and if possible, electronic access to data and information under the purview of the SAF/IG that is necessary to evaluate risk and identify, analyze, and resolve or clarify insider threat matters. Data and information include, but is not limited to, relevant law enforcement, counterintelligence, and inspector general data and information.

3.11. **Director Legislative Liaison (SAF/LL)** will support SAF/OC, SAF/AQ, SAF/SQ with congressional interactions, as required.

3.12. **Director, Administration and Management, Office of the Secretary (SAF/AM) and Deputy Chief Management Office (DCMO)** will develop, disseminate, and implement policy and guidance to ensure compliance with regulations regarding privacy and civil liberties and the DAF business mission area programs.

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

3.13.1. Inform SAF/OC on suitability and fitness policies for employment and common access card credentialing, for civilian and military personnel.

3.13.2. Define 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.

3.13.3. Ensure procedures are established with the C-InTP to allow regular, timely, and if possible, electronic access to data and information under the purview of SAF/MR that is necessary to evaluate risk, and identify, analyze, and resolve or clarify Insider Threat matters.

3.13.4. Monitor and integrate applicable policy and guidance related to personnel security processes, systems, and procedures for the Non-Sensitive Public Trust (NSPT)population enrolled in continuous vetting.

3.13.5. Oversee and conduct PPBE activities for the NSPT population enrolled in continuous vetting and ensure resources are established and sustained.

3.14. **Director, DAF Studies and Analysis (SAF/SA)** is responsible for advising DAFSE decisions with decision-quality analysis.

3.15. **Air Force Surgeon General (AF/SG)** will:

3.15.1. Serve as a technical advisor to provide input in DAFSE policies and procedures as it relates to protected health information and force health protection.

3.15.2. Provide support to the Presidential Support Program and Yankee White nomination process through medical certifications of members nominated for presidential support duties.

3.16. **Executive Director, Test and Evaluation (AF/TE)** is responsible for guidance, direction, and oversight of matters affecting test equities for SAP activities and serves as the lead for the foreign materiel program for the DAF.

3.17. **Deputy Chief of Staff for Manpower, Personnel and Services (AF/A1) and Space Force Chief Human Capital Officer (SF/CHCO) (SF/S1)** will:

3.17.1. Oversee security civilian and military certification, training, and position identification in appropriate databases.

3.17.2. Define policy and guidance for integrating and vetting emerging institutional security education and training requirements or learning outcomes into accessions, professional military education, professional continuing education, and ancillary training.

3.17.3. Support manpower requirements, allocations, and personnel assignments for SAPs and information protection.

3.18. **Deputy Chief of Staff, Intelligence, Surveillance, Reconnaissance, and Cyber Effects Operations (AF/A2/6) and Deputy Chief of Space Operations for Intelligence (SF/S2)** will:

3.18.1. Serve as the Head of the Intelligence Community (IC) Element, responsible for the oversight, management, security, and administration of the SCI program. Responsibilities for these requirements are identified in Section 1.6 of E.O. 12333, *United States Intelligence Activities*.

3.18.2. Integrate requirements for the security, use, and dissemination of SCI and associated SCI policy into DAFSE security programs. These requirements will consider Intelligence Community Directive (ICD) 906, *Controlled Access Programs*, ICD 700, *Protection of National Intelligence*, DoDD 5148.13, *Intelligence Oversight*, DoD Manual (DoDM) 5105.21 Vol 1, *Sensitive Compartmented Information*, DoDM 5105.21 Vol 2, *Administration of Physical Security, Visitor Control, and Technical Security*, and DoDM 5105.21 Vol 3, *Administration of Personnel Security, Industrial Security, and Special Activities*, as well other policies that may impact the DAFSE.

3.18.3. Oversee acquisition intelligence support (i.e., intelligence mission databases).

3.18.4. Serve as the IC Element authority for Controlled Access Programs (CAP).

3.18.5. Establish procedures for foreign disclosure of military and national intelligence within the DAFSE as reflected in DAFMAN 16-201, Department of the Air Force Foreign Disclosure and Technology Transfer Program; DoDD 5230.11, Disclosure of Classified Military Information to Foreign Governments and International Organizations; and ICD 403, Foreign Disclosure and Release of National Intelligence. Coordinate with SAF/IA to ensure military and national intelligence equities and procedures are included in broader DAF disclosure processes and guidance.

3.19. **Deputy Chief of Staff, Operations (AF/A3) and Space Force Chief Operations Officer (SF/COO)** will:

3.19.1. In coordination with SAF/OC, integrate Operations Security (OPSEC), and air, space, and cyberspace operations policy, guidance, and procedures within the DAFSE.

3.19.2. Synchronize security enterprise and mission assurance efforts with the warfighting mission area.

3.19.3. Serve as component Integrated Joint Special Technical Operations (IJSTO) lead for conducting SAP operations, planning, integration, training, and readiness to execute warfighting capabilities.

3.20. **Deputy Chief of Staff for Logistics, Engineering, and Force Protection (AF/A4) and SF/COO** will:

3.20.1. Integrate Physical Security, Force Protection, Logistics, and Civil Engineering policy, guidance, and procedures within the DAFSE.

3.20.2. In coordination with AFOSI, ensure procedures are established to securely share law enforcement and other applicable information consistent with privacy laws, civil liberties, and regulations with authorized C-InTP personnel to identify, analyze and resolve insider threat issues.

3.20.3. Integrate Physical Security and Force Protection guidance and procedures into C-InTP for both prevention and response.

3.20.4. In coordination with the DAF SAPCO, provide policy implementation guidance to SAP logistics, engineering, chemical/biological/radiological/nuclear defense, emergency management, and force protection activities.

3.21. **Deputy Chief of Staff, Air Force Futures (AF/A5/7) and Space Force Chief Strategy and Resourcing Officer (CSRO) (SF/S5/8)** will:

3.21.1. Manage and validate SAP requirements through the Joint Capabilities, Integration, and Development System.

3.21.2. In coordination with AF/A8 integrate SAPs into long-range strategic plans and the Program Objective Memorandum through corporate process special sessions, in coordination with the appropriate stakeholders.

3.22. **Deputy Chief of Staff, Plans and Programs (AF/A8) and SF/S5/8** will prioritize SAP and non-SAP programmatic adjustments proposed during budget deliberations and during the SECDEF's Program Budget Review process.

3.23. **Deputy Chief of Staff for Strategic Deterrence and Nuclear Integration (AF/A10) and SF/COO** will:

3.23.1. Serve as the DAF OPR for the Unclassified Controlled Nuclear Information program in coordination with AF/A4.

3.23.2. Integrate nuclear deterrence mission policies and procedures into DAFSE procedures, to ensure protection of nuclear weapons and nuclear operations.

3.23.3. Provide subject matter expertise on the classification and/or declassification of restricted data, formerly restricted data, controlled nuclear weapons design information, Department of Energy Sigma information, and transclassified foreign nuclear information.

3.23.4. In coordination with the DAF SAPCO, provide guidance and oversight of SAP activities with nuclear and strategic deterrence equities, as well as counter-proliferation, nonproliferation, countering weapons of mass destruction, and chemical, biological, radiological, and nuclear issues.

3.23.5. In coordination with SAF/OC, oversee formulation of guidance and help protect U.S. national security information in the negotiation, inspection, verification, and compliance of treaties and other international obligations, including arms control and nonproliferation agreements.

3.24. **Air Force Rapid Capabilities Office (AFRCO) and Space Rapid Capabilities Office (SpRCO)** will advise and assist the SecAF and USecAF with daily management, strategic planning and programming, acquisition efforts, and life cycle management to execute roles and responsibilities outlined in the AFRCO and SpRCO charters for assigned DoD SAPs.

3.25. **MAJCOM, FLDCOM, Direct Reporting Unit (DRU), and Field Operating Agency (FOA) Commander/Director** will:

3.25.1. Ensure all DAF personnel (military, civilian, and contractor support) are trained on their personal responsibility to adhere to security requirements.

3.25.2. Ensure proper implementation of security is directed by commanders and other leaders at every level and is fostered through Security Education, Training, and Awareness, and leadership.

3.25.3. Appoint a SPE, in writing. The SPE will be the Vice (or Deputy) Commander, who has knowledge of security disciplines within the command's security enterprise necessary to facilitate and oversee implementation of the command's security framework and strategic plan.

3.25.4. Establish an Information Protection directorate and appoint, in writing, a Director of Information Protection (DIP) of appropriate civilian grade to interact with and provide authoritative IP guidance to senior DAF and outside agency leadership. The DIP will serve as the single focal point for policy, management, security, data collection, metrics, coordination, dissemination, and reporting of collateral security functions. The DIP will:

3.25.4.1. Collaborate with MAJCOM A1 and FLDCOM/S1 to determine the appropriate manpower and resources necessary for their staffs and installation IP offices and advise installation commanders on prospective IP office candidate qualifications.

3.25.4.2. Provide IP security subject matter expertise to MAJCOM/ FLDCOM IG for IP inspections as prescribed in DAFI 90-302, *The Inspection System of the Department of the Air Force*. Conduct IP security compliance inspections of subordinate organizations.

3.25.4.3. Assure completion of annual program data calls and other applicable program reporting requirements.

3.25.5. Facilitate coordination and collaboration among Information Protection, SAP, and SCI security functions to ensure effective and efficient program operations. Commanders are encouraged to foster an environment where distinct security disciplines share information and collaborate as appropriate, to enhance the overall security posture and operational effectiveness.

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

3.25.7. Establish a Special Access Program Management Office (SAPMO) and appoint, in writing, a director of appropriate rank or civilian grade to interact with and provide authoritative SAP guidance to senior DAF and outside agency leaders. (**Exception**: FOAs will not establish a SAPMO). DRUs are not required to establish a SAPMO, but may do so if they support a SAP mission. Under the director, the SAPMO will serve as the single focal point to the DAF SAPCO for policy, management, security, coordination, dissemination, and reporting of all SAP activities in which the command participates to include:

3.25.7.1. Determine the appropriate manpower and resources necessary for their respective SAPMO and resource appropriately, to include appointing, in writing, a command Government SAP Security Officer (GSSO). Examples of additional SAP manpower positions directors may consider include, but are not limited to, cybersecurity; logistics/maintenance; or technical advisor.

3.25.7.2. Conduct SAP security compliance inspections of subordinate organizations in accordance with DoDM 5205.07. Coordinate with and provide SAP security subject matter expertise to MAJCOM/FLDCOM IG for SAP inspections as prescribed in DAFI 90-302, *The Inspection System of the Department of the Air Force.*

3.25.7.3. Adhere to and ensure compliance with SAF/CN reporting requirements (i.e., Federal Information Security Modernization Act, Clinger-Cohen Act of 1996) for SAP information systems owned by their organizations.

TROY E. MEINK
Secretary of the Air Force

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

40 USC § 11101 (3), *Clinger-Cohen Act of 1996*

44 USC § 3554, *Federal Agency Responsibilities*

AFI 33-322, *Records Management and Information Governance Program,* 23 Mar 20

AFPD 16-7, *Special Access Programs,* 21 Nov 17

AFPD 90-6, *Air Force Strategy, Planning, Programming, Budgeting, and Executions (SPPBE) Process,* 26 Jun 19

AFRCO *Charter,* 13 Aug 18

AFMAN 16-1406 Vol 2_DAFGM2025-01, *National Industrial Security Program: Industrial Security Procedures for Government Activities,* 20 Feb 25

AFI 16-701, *Management, Administration and Oversight of Special Access Programs,* 18 Feb 14

CJCSI 3120.08E, *Integrated Joint Special Technical Operations,* 11 March 2025

DAFGM2024-16-1410, *Department of the Air Force Enhanced Security Program to Support the DoD Innovation Initiative,* 20 Jun 24

DAFH 16-1406, *National Interest Determinations,* 16 Mar 23

DAFI 16-1401, *Information Protection Program,* 3 Feb 23

DAFI 16-1402_DAFGM2025-01, *Counter-Insider Threat Program Management,* 25 Feb 25

DAFI 16-1403_DAFGM2024-01, *Controlled Unclassified Information (CUI),* 26 Nov 24

DAFI 63*Defense Federal Acquisition Regulation Supplement,* current edition

Department of the *Air Force Federal Acquisition Regulation Supplement,* current edition

DoDD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations,* 7 November 2023

DoDI5000.83_DAFI63-113, *Technology and Program Protection to Maintain Technological Advantage,* 08 Mar 22

DAFMAN 16-1404 Vol 1_DAFGM2024-01, *DoD Information Security Program: Overview, Classification, and Declassification,* 27 Aug 24

DAFMAN 16-1404 Vol 2, *Information Security Program: Marking of Information,* 7 Jan 21

DAFMAN 16-1404 Vol 3, *Information Security Program: Protection of Classified Information,* 17 Apr 22

DAFMAN 16-1405_DAFGM2024-01, *Department of the Air Force Personnel Security Program,* 26 Nov 24

DAFMAN 16-101, *Security Cooperation (SC) and Security Assistance (SA) Management,* 13 Dec 24

DAFMAN 16-201, *Department of the Air Force Foreign Disclosure and Technology Transfer Program,* 19 Jan 21

DAFMAN 90-161, *Publishing Processes and Procedures,* 15 Apr 22

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

DoDD 5205.07, *Special Access Program (SAP) Policy*, 1 Jul 10

DoDI 5205.16, *The DoD Insider Threat Program*, 20 December 2024

DoDD 5210.48, *Credibility Assessment (CA) Program*, 24 Apr 15

DoDD 5210.50, *Management of Serious Security Incidents Involving Classified Information*, 27 Oct 14

DoDD 5210.55, *Department of Defense Presidential Support Program*, 15 Dec 98

DoDI 2000.25, *DoD Procedures for Reviewing and Monitoring Transactions Filed with the Committee on Foreign Investment in the United States*, 27 May 22

DoDI 5200.01, *DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI),* 21 Apr 16

DoDI 5200.02, *DoD Personnel Security Program (PSP),* 21 Mar 14

DoDI 5205.11, *Management, Administration, and Oversight of DoD Special Access Programs (SAPs),* 12 Sept 24

DoDI 5205.85, *Enhanced Security Program to Support the DoD Innovation Initiative*, 16 Aug 22

DoDI 5210.87, *Selection of DoD Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities (PSAs),* 30 Nov 98

DoDI 5220.31, *National Industrial Security Program (NISP)*, 9 May 2023

EO 13526, *Classified National Security Information*, 29 Dec 2009

EO 13556, *Controlled Unclassified Information*, 4 Nov 2010

Federal Acquisition Regulation, *current* edition

HAFMD 1-12, *Assistant Secretary of the Air Force (Financial Management and Comptroller),* 13 Jun 23

HAFMD 1-52, *Director of Test and Evaluation,* 20 Apr 21

HAFMD 1-56, *Deputy Chief of Staff Plans and Programs,* 3 Dec 19

HAFMD 1-57, *Deputy Chief of Staff, Air Force Futures*, 17 Aug 23

HOI 65-6, *Insider Threat Resource Governance and Management Process*, 11 May 18

National Security Presidential Memorandum 28, *The National Operations Security Program,* 13 Jan 2021

HQDAFMD 1-15, *Director, Office Competitive Activities*, 23 Jan 25

SpRCO Charter, 9 Aug 19

AFI 10-701, *Operations Security (OPSEC),* 9 June 2020

Prescribed Forms

None

Adopted Forms

DAF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AFI—Air Force Instruction

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

AFRCO—Air Force Rapid Capabilities Office

DAFSEEB—Department of the Air Force Security Enterprise Executive Board

CA—Credibility Assessment

CAP—controlled access program

CJCSI—Chairman of the Joint Chiefs of Staff Instruction

CUI—Controlled Unclassified Information

C-InT—Counter-Insider Threat

C-InTP—Counter-Insider Threat Program

CSAF—Chief of Staff of the Air Force

CSO—Chief of Space Operations

CV—Continuous Vetting

DAF—Department of the Air Force

DAFMAN—Department of the Air Force Manual

DAFPD—Department of the Air Force Policy Directive

DAF SAPCO—Department of Air Force Special Access Program Central Office

DAFSE—Department of the Air Force Security Enterprise

DEPSECDEF—Deputy Secretary of Defense

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DoDM—Department of Defense Manual

DoD SAPCO—Department of Defense Special Access Program Central Office

DRU—Direct Reporting Unit

DSE—Defense Security Enterprise

DSE EXCOM—Defense Security Enterprise Executive Committee

E.O.—Executive Order

FLDCOM—Field Command

FOA—Field Operating Agency

GAM—Government Activity Manager

GSSO—Government SAP Security Officer

HAF—Headquarters Air Force

IC—Intelligence Community

IG—Inspector General

IP—Information Protection

JSIG—Joint Special Access Program Implementation Guide

MAJCOM—Major Command

NISP—National Industry Security Program

OCA—Original Classification Authority

OPR—Office of Primary Responsibility

OPSEC—Operations Security

POM—Program Objectives Memorandum

PPBE—Planning, Programming, Budgeting, and Execution

PSI—Personnel Security Investigations

PSP—Personnel Security Program

SAF—Secretary Air Force

SAP—Special Access Program

SAPCO—Special Access Program Central Office

SAPMO—Special Access Program Management Office

SAPOC—Special Access Program Oversight Committee

SecAF—Secretary of the Air Force

SECDEF—Secretary of Defense

SETA—Security Education, Training and Awareness

SCI—Sensitive Compartmented Information

SF—Space Force

SPE—Security Program Executive

SpRCO—Space Rapid Capabilities Office

SSWG—Department of the Air Force Special Access Program Senior Working Group

US—United States

USC—United States Code

USecAF—Under Secretary of the Air Force

VCSO—Vice Chief of Space Operations

VCSAF—Vice Chief of the U.S. Air Force

Office Symbols

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

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

AF/A3—Deputy Chief of Staff, Operations

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

AF/A5/7—Deputy Chief of Staff for Strategy, Integration, Requirements, and Plans

AF/A8—Deputy Chief of Staff for Programs

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

AF/SG—Air Force Surgeon General

AF/JA—Air Force Judge Advocate

SAF/AG—Auditor General of the Air Force

SAF/AM—Administration and Management

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

SAF/AQL—Special Programs

SAF/CN—Office of the Chief Information Officer

SAF/FM—Assistant Secretary of the Air Force for Financial Management and Comptroller

SAF/GC—General Counsel of the Air Force

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

SAF/IE—Assistant Secretary of the Air Force for Installations, Environment, and Energy

SAF/IG—Inspector General of the Air Force

SAF/LL—Assistant Secretary of the Air Force for Legislative Liaison

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

SAF/OC—Office of Competitive Activities

SAF/OCS—Special Security Directorate

SAF/SA—Director, Office of Studies and Analysis

SAF/SQ—Assistant Secretary of the Air Force for Space Acquisition and Integration

SAF/SQXL—Assistant Secretary of the Air Force for Space Acquisition and Integration, Special Programs Division

AF/TE—Director, Air Force Test and Evaluation

SF/COO—Chief Operations Officer

SF/CHCO—Chief Human Capital Officer

SF/CSRO—Chief Strategy and Resourcing Officer

SF/S1—Chief Human Capital Office

SF/S2—Deputy Chief of Space Operations for Intelligence

SF/S5/8—Chief Strategy and Resourcing Office

AFOSI—Air Force Office of Special Investigations

AFOSI PJ—Air Force Office of Special Investigations, Office of Special Projects

AFRCO—Air Force Rapid Capabilities Office

SpRCO—Space Rapid Capabilities Office

Terms

Carve-out—A provision approved by the Secretary or Deputy Secretary of Defense that relieves the Defense Counterintelligence Security Agency of its National Industrial Security Program obligation to perform Industrial Security oversight functions for a Department of Defense Special Access Program.

Controlled Access Program (CAP)-—Special Access Program pertaining to intelligence sources, methods, and activities exercised by the Director of National Intelligence as identified in Section 4.3 of Executive Order (E.O.) 13526, *Classified National Security Information.*

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.

Counter-Insider Threat—Functions and activities consisting of the full range of measures employed by DoD Components to detect, deter, and mitigate risks and prevent the potential threats insiders may pose to DoD installations, facilities, personnel, missions, or resources. This includes prevention and deterrence efforts amongst workplace violence programs, mitigation of risk for potentially violent behavior through prevention, assistance, and response capabilities, unauthorized disclosure programs, Hub operations, and other risk or threat management capabilities.

DAF Counter-Insider Threat Hub—A centralized DAF capability that collects, aggregates, reviews, and assesses information derived from counterintelligence, security, information assurance, human resources, law enforcement, IG, user activity monitoring, and other applicable sources to inform Commanders and senior leaders of holistic risk and recommend mitigation measures to address and lower risk.

Credibility Assessment—The overarching term covering programs, research, training, and procedures that employ technologies to assess an individual's truthfulness with the aid of technical devices that measure physiological data or behavioral activity.

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.

Government Activity Manager—The appointed individual responsible for managing assigned SAP(s). The GAM assumes the responsibility for overall security management of assigned SAPs. Often, the GAM is the organization's commander or director, though not always.

Industrial Security—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 E.O. 13526 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security. The term also applies to policies, procedures and requirements established to protect Controlled Unclassified Information, which may be withheld from release to the public in accordance with statute, regulation, or policy.

Insider Threat—A threat presented by a person who has, or once had, authorized access to information, a facility, network, a person, or a resource of the DoD and wittingly or unwittingly commits an act in contravention of law or policy that resulted in or might result in harm through the loss or degradation of government or company information, resources, or capabilities or a destructive act, which may include physical harm to one's self or another in the workplace.

Original Classification Authority—An individual authorized in writing, either by the President, Vice President, or by agency heads or other officials designated by the President, to originally classify information (i.e., to classify information in the first instance).

Oversight—Authority to monitor, review, analyze, and advise 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—Policies, practices and procedures that ensure 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.

Program Security—A SAP centric Counterintelligence and Acquisition Security-based competency that employs an array of enhanced protection requirements for highly sensitive United States Government programs/capabilities that maintain U.S. technological advantages, vulnerabilities, and/or highly sensitive intelligence or operational plans and if compromised could cause significant degradation to U.S. warfighting advantages and national security. Program Security employs security processes centered on a valid Need-to-Know (NTK) and material contribution criteria separate and distinct from collateral and Sensitive Compartmented Information (SCI). The enhanced security measures are applied contract security measures,

personnel access, Program Protection Plans, supply chain risk mitigation, system protection, and Foreign Ownership, Control, or Influence (FOCI) review tailored to the specific programs/capabilities. Such forms the basis for the protection of SAP Information throughout the contract lifecycle.

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 against 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 Enterprise—The framework for integrating Personnel, Industrial, Information, Physical and Operations Security, Operations Security, Special Access Program security, Controlled Unclassified Information, Critical Program Information (CPI) 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 Offices, Special Access Programs, and Cybersecurity entities to inject IP elements into security planning into daily and ongoing missions, such as OPSEC 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/OC; at the MAJCOM, FLDCOM, DRU, and FOA, this is the vice (or deputy) commander.

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.

Special Access Program—A security program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

Attachment 2

DAF SAP GOVERNANCE STRUCTURE

A2.1. The DAF SAP governance structure is used to manage and oversee DAF SAP equities on behalf of the SecAF. All SAPs for which the DAF exercises cognizant authority, or in which the DAF is a stakeholder, will be managed by the DAF SAP governance structure, consistent and aligned with the DoD's SAP governance structure. As such, the DAF's SAP governance structure will consist of the DAF SAP Oversight Committee (SAPOC) and the DAF SAP Senior Working Group (SSWG).

A2.2. The DAF SAPOC is the executive level senior governing body of the DAF SAP Enterprise for governance, management, and oversight of SAPs under DAF cognizance. It supports the DoD SAPOC governance architecture to ensure SAPs meet warfighter needs while protecting CPI.

A2.2.1. The SecAF and USecAF lead the DAF SAPOC, and the USecAF shall represent the DAF at the DoD SAPOC. The Director, DAF SAPCO is assigned the role of DAF SAPOC Executive Secretary. Members of the DAF SAPOC include:

A2.2.1.1. CSAF

A2.2.1.2. CSO

A2.2.1.3. VCSAF

A2.2.1.4. VCSO

A2.2.1.5. Additional attendees may be invited at the discretion of the SecAF or USecAF based on specific topic requirements.

A2.2.2. The DAF SAPOC shall:

A2.2.2.1. Review the status, execution, management, and protection level of SAPs for which the DAF has cognizance, as required.

A2.2.2.2. Review compliance status of SAPs for which the SecAF has cognizant authority or SAPs in which the DAF is a stakeholder.

A2.2.2.3. Review any additional DAF-level SAP topics for discussion at the DoD SAPOC.

A2.2.2.4. Meet as necessary, when convened by the SecAF or USecAF, to resolve DAF SAP concerns elevated by the DAF SSWG, or in preparation for the DoD SAPOC.

A2.3. The DAF SSWG is the working-level governance, collaboration, and action body of the DAF SAP Enterprise. It will advise and assist the SecAF, the USecAF, and the DAF SAPOC by executing the DAF corporate governance, management, and oversight responsibilities for SAPs, over which SecAF has cognizant authority or in which the DAF is a stakeholder.

A2.3.1. Members of the DAF SSWG include:

A2.3.1.1. Director, SAF/OCS (Chair)

A2.3.1.2. Director, SAF/AQL

A2.3.1.3. Director, AFRCO

A2.3.1.4. Director, AFOSI PJ

A2.3.1.5. Director, SAF/SQXL

A2.3.1.6. Director, SpRCO

A2.3.1.7. Additional attendees may be invited at the discretion of SAF/OCS based on specific topic requirements.

A2.3.2. The DAF SSWG Shall:

A2.3.2.1. Execute governance, oversight and synchronization of all DoD SAPs assigned to the DAF on behalf of the DAF SAPOC.

A2.3.2.2. Review compliance status of SAPs for which the SecAF has cognizant authority or SAPs in which the DAF is a stakeholder.