BY ORDER OF THE
SECRETARY OF THE AIR FORCE

HEADQUARTERS DEPARTMENT OF THE
AIR FORCE MISSION DIRECTIVE 1-15

23 JANUARY 2025

DIRECTOR, OFFICE OF
COMPETITIVE ACTIVITIES

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This publication is available for downloading or ordering on the e-Publishing website at **www.e-Publishing.af.mil**.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/OC

Certified by: SAF/OC
(Mr. Edwin H. Oshiba)

Pages: 12

This publication includes significant changes to the role, responsibility, and organizational adjustments to reflect the separation and realignment of Administrative Assistant to the Secretary of the Air Force (SAF/AA), stand-up of the Office of Administration and Management (SAF/AM) and the Office of Competitive Activities (SAF/OC). This publication supersedes portions of HAFMD 1-6, *Administrative Assistant to the Secretary of the Air Force*, 22 December 2014. It also rescinds any SAF/AA roles and responsibilities as the Air Force Restricted Data Management Official (RDMO) as set forth in HAFMD 1-6, HAFMD 1-60, *Deputy Chief of Staff of the Air Force (Strategic Deterrence and Nuclear Integration)*, 6 December 2019, Air Force Policy Directive 13-5, *Air Force Nuclear Mission*, 17 July 2018 and any other Department of the Air Force (DAF) publications that contain conflicting guidance regarding RDMO.

1. Mission. Pursuant to Title 10 United States Code (U.S.C.) §§ 9013-9016, the Secretary of the Air Force (SecAF) may establish offices and officials within the Office of the Secretary of the Air Force (known as the Secretariat) to assist in carrying out their responsibilities. As documented by Paragraph 4.1. of Air Force Mission Directive 1, *Headquarters Air Force (HAF)*, and this Headquarters Department of the Air Force Mission Directive (HQ DAFMD), the Director of the Office of Competitive Activities (SAF/OC) is established as part of the Secretariat. The SAF/OC has overall responsibility for managing DAF, security enterprise to include information security, personnel security, industrial security, counter insider threat program, Presidential Support Program, and special access programs (SAPs). SAF/OC manages policy, oversight and integration of all competitive activities; as well as managing and preparing policies for DAF sensitive

activities; and manages and oversees programs and activities identified and directed by the SecAF. SAF/OC has overall responsibility for fostering perception management of DAF capabilities through synchronized sensitive activities and mission-integrated information security policies; facilitating synchronization of disparate, competitive activities occurring across the DAF; collaborating with other Military Services, Combatant Commands (CCMD), Office of the Secretary of Defense (OSD) (to include Defense Agencies), and interagency partners to create synergistic effects; and facilitation of coherent assessments, planning, resource advocacy, and oversight of synchronized strategic messaging and competitive activities. The SecAF retains ultimate responsibility for all policies related to the DAF. Within their areas of responsibility, the SAF/OC develops and approves policies and programs, issues official guidance via Department level publications, and oversees the implementation and execution of those policies and programs.

2. Organizational Relationships. Subject only to the authority, direction, and control of the Secretary of Defense, the SecAF is responsible for, and has all legal authority necessary to conduct the affairs of the DAF. The Secretariat, Air Staff and Space Staff perform their DAF functions subject to statutory authority and the authority, direction and control of the SecAF.

2.1. The SAF/OC reports to the SecAF, serves as an agent of SecAF within assigned policy and program domains, and provides guidance, direction, and oversight for all matters pertaining to the formulation, review, and execution of plans, policies, programs, and budgets within their area of responsibility. The SAF/OC is accountable to the Secretary for results achieved within the policy and program domains, assigned by this Directive.

2.2. The SAF/OC and the Office of the SAF/OC work in cooperation with the Chief of Staff of the Air Force, Chief of Space Operations, Vice Chief of Staff of the Air Force, Vice Chief of Space Operations, the Under Secretary of the Air Force (USecAF), the Assistant Secretaries of the Air Force, Air Staff and Space Staff and their respective offices, as well as other Headquarters DAF (HQ DAF) organizations, which are responsible, pursuant to Chapters 903, 905, and 908 of Title 10 U.S.C. (Sections 9011-9024, 9031-9040, and 9081-9086), for assisting the SecAF in carrying out his/her responsibilities.

2.2.1. Pursuant to Headquarters Operating Instruction (HOI) 90-1, *Headquarters Air Force Mission Directives and Department of Defense Issuances Programs*, two or more HQ DAF two-letter organizations with responsibilities in the same functional area will develop "Standard Operating Procedures (SOPs)" that set forth procedures enabling covered organizations to fulfill and carry out their respective missions, roles, and responsibilities. Any SOPs entered into by the SAF/OC will be included at **Attachment 3** of this publication.

3. Responsibilities. The SAF/OC is specifically responsible for:

3.1. Advising the SecAF on all matters pertaining to competitive activities strategic planning, assessments, and resourcing supporting enterprise competition priorities, as well as, informing enterprise-level decisions for the DAF.

3.2. Providing policy, oversight, and guidance of competitive activities across the DAF, which include activities related to DAF Operations, Activities, and Investments (OAIs) that by design shift the focus of strategic competition into areas that favor DAF interests and functions.

3.3. Leading the coordination and synchronization of DAF competitive activities.

3.4. Establishing and leading DAF competitive activities governance councils, boards, and groups.

3.5. Establishing DAF processes providing integrated assessments, campaign and mission-specific plans, and competitive effects.

3.6. Facilitating collaboration with other Military Services, Joint Staff, Combatant Commands (CCMDs), OSD (to include Defense Agencies), and interagency partners to enable DAF enterprise competitive efforts. Serving as focal point for DAF competitive activities equities for Congress, OSD (Strategic Information Oversight Board (SIOB)), Joint Staff, CCMDs, Services, industry, academia, and United States allies and partners.

3.7. Serving as the functional advocate for competitive activities programs and initiatives.

3.8. Issuing guidance to provide for the coordination of, and decision-making for, the planning, programming, and control of investments in competitive activities portfolio management.

3.9. Coordinating with 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) on matters pertaining to acquisition of competitive activities capabilities and capabilities development.

3.10. Leading competitive activities assessments across air, space, and cyberspace to inform DAF enterprise-level decisions.

3.11. Departmental policy formulation for DAF cover programs.

3.12. Performs the role and responsibilities of the DAF SAP cognizant authority (CA) consistent with Department of Defense Directive (DoDD) 5205.07, *DoD Special Access Program Policy,* and DoD Instruction (DoDI) 5205.11, *Management, Administration, and Oversight of DoD Special Access Programs (SAPs)*. Providing policy, direction, administration, oversight and implementation of DAF SAP.

3.13. Establishing and overseeing a DAF Special Access Program Central Office (SAPCO) and designating a SAPCO Director, which may include a SAPCO for the Air Force and Space Force. When directed, the DAF SAPCO (also known as the CA SAPCO as found in DoDI 5205.11) shall be responsible for developing and implementing policies and procedures for the execution, management, oversight, administration, security, data protection and records management for SAPs. SAPs exercised under the authority of the DNI that pertain to intelligence sources, methods, and activities (also known as Controlled Access Programs defined in ICD 906) are separately managed and administered by the Heads of the Intelligence Community Elements (HICE) for the Air Force and Space Force. Oversight of intelligence and intelligence-related DAF SAPs will be coordinated with the appropriate Service HICE to ensure compliance with EO 12333, *United States Intelligence Activities,* DoDD 5148.13, *Intelligence Oversight*.

3.14. Departmental policy formulation for SAP security oversight for international arms control agreements and treaty issues.

3.15. Oversight and coordination of DAF and DAF-supported sensitive activities; serve as the senior Sensitive Activities Official for the DAF.

3.16. Providing career field leadership, policy, guidance, and oversight for select military and civilian personnel, based on the unique mission, and associated security classification, requirements, and limitations, that support DAF and DAF-supported sensitive and special activities.

3.17. Consistent with applicable statutory authorities, oversight of DAF personnel assignments for SAPs and other sensitive activities.

3.18. Oversight of and implementation of the DAF Insider Threat Program; serve as the senior official of the DAF Counter Insider Threat Program (C-InTP) providing policy, oversight, and management of the program; advocate for resources necessary for the DAF C-InTP.

3.19. Serving as the DAF Senior Agency Official and the Security Program Executive with oversight and management responsibilities for the DAF Security Enterprise (DAFSE). Integrates with other two-letter offices on security plans, policies, programs, resources, information sharing and risk management activities. Chairs the DAF Security Enterprise Executive Board (DAFSEEB).

3.20. Representing the DAFSE at the Defense Security Enterprise Executive Committee.

3.21. Oversight of assigned responsibilities, roles, and functions regarding sensitive activities as delegated to the SecAF pursuant to memoranda of understanding/agreement with the Office of the Under Secretary of Defense for Intelligence & Security (OUSD (I&S)) consistent with direction from the Secretary of Defense.

3.22. Executing roles and responsibilities for operations, sustainment, and modernization of DoD Mission Partner Environment (MPE) enterprise capabilities pursuant to DoDD 5101.22E *DoD Executive Agent (DoD EA) for DoD Mission Partner Environment (MPE)* and DoDI 8110.01, *Mission Partner Environment Information Sharing Capability Implementation for the DoD*, in support of individual program sponsors, and in coordination the DoD MPE EA and offices executing the duties of the DoD MPE EA.

3.23. Coordination with the USAF and USSF Intelligence Community Elements' respective cognizant security authorities for the protection of national intelligence and intelligence sources, methods, and activities to include Sensitive Compartmented Information (SCI).

4. Delegations of Authority/Assignment of Responsibility: **Attachment 1** lists authorities delegated and responsibilities assigned by the SecAF to the SAF/OC. The authorities delegated/responsibilities assigned to the SAF/OC by this HQ DAFMD may be re-delegated or reassigned to other DAF officials unless re-delegation is expressly prohibited by the attached delegation or by controlling law, regulation, or DoD issuance. While the SAF/OC may re-delegate authorities or reassign responsibilities, he/she will ultimately be responsible to the SecAF for all matters listed in Paragraph **1** and **3** of this publication. Any re-delegation of authority/assignment of responsibility shall not be effective unless it is in writing, has been reviewed by the office of the General Counsel of the Department of the Air Force as the primary legal advisor and the Office of the Judge Advocate General of the Air Force may provide complimentary legal advice, and is signed by the Director of SAF/OC. Any person re-delegating authority in accordance with this HQ DAFMD may further restrict or condition the authority/assignment of responsibility being re-delegated/reassigned.

5. Notifications to Congress: No re-delegation of authority/assignment of responsibility under this HQ DAFMD below the level of a Deputy Assistant Secretary or three-letter/digit office shall include authority to provide notifications or reports to Congress.

6. Continuation of Prior Re-Delegations of Authority/Assignments of Responsibility. Re-delegations of authority/assignments of responsibility made prior to the date of issuance of this HQ DAFMD remain effective, insofar as such re-delegations are not inconsistent with the terms of this HQ DAFMD unless superseded by a new re-delegation or assignment of responsibility.

FRANK KENDALL
Secretary of the Air Force

Attachments:
1. Delegations of Authority/Assignments of Responsibility for SAF/OC
2. Organizational Chart/Three-Letter Responsibilities

Attachment 1

DELEGATIONS OF SECRETARY OF THE AIR FORCE AUTHORITY/ ASSIGNMENTS OF RESPONSIBILITY

TO THE

DIRECTOR FOR THE OFFICE OF COMPETITIVE ACTIVITIES

A1.1. Responsibility relating to United States security authority for North Atlantic Treaty Organization (NATO) affairs, as delegated to the SecAF, pursuant to DoDD 5100.55, *United States Security Authority for North Atlantic Treaty Organization Affairs (USSAN)*.

A1.2. Authority relating to reporting DoD intelligence and intelligence-related sensitive activities, other than Counterintelligence (CI) and Human Intelligence (HUMINT) activities, for the preceding fiscal quarter to the Office of the Under Secretary of Defense, Intelligence and Security, Sensitive Activities Directorate, as delegated to the SecAF, pursuant to DoDI O-5100.94, *Oversight, Coordination, Assessment, and Reporting of DoD Intelligence and Intelligence-Related Sensitive Activities*.

A1.3. Authority relating to DoD cover and cover support activities, as delegated to the SecAF, pursuant to DoDD S-5205.61, *DoD Cover and Cover Support Activities*.

A1.4. Authority relating to the implementation of DoD cover and cover support activities as delegated to SecAF pursuant to DoDI S-5105.63, *Implementation of DoD Cover and Cover Support Activities (U)*.

A1.5. Authority relating to the implementation of DoD cover and cover support activities in cyberspace as delegated to SecAF pursuant to DoDI S-5205.84, *DoD Cover and Cover Support Activities in Cyberspac*e.

A1.6. Responsibility relating to DoD security training and authority to appoint a representative to the DoD Security Training Council, as delegated to the SecAF, pursuant to DoDI 3305.13, *DoD Security Education, Training, and Certification*.

A1.7. Responsibility to provide to the General Counsel of the Department of Defense (GC DoD), or GC DoD's designee, information and recommendations related to execution of GC DoD's responsibilities pursuant to DoDI 5145.03, *Oversight of the DoD Personnel Security Programs*.

A1.8. Responsibility relating to DoD Personnel Vetting Program (excluding the adjudication and background investigations of DAF personnel security clearances), with the exception that the Assistant Secretary of the Air Force for Manpower and Reserve Affairs oversees the DAF Personnel Security Appeals Board, as delegated to the SecAF, pursuant to DoDI 5200.02, *DoD Personnel Security Program (PSP*). Adjudication authority resides with the Defense Counterintelligence and Security Agency Adjudicative Vetting Services (AVS), formerly the DoD Consolidated Adjudication Services (CAS).

A1.9. Responsibility relating to the direction, administration, and oversight of the Department of the Air Force's Security Program, as delegated to the SecAF, with the exception of the Sensitive Compartmented Information Security Program, including the protection of all national intelligence and intelligence sources, methods, and activities, pursuant to DoDI 5200.01, *DoD Information Security Program and Protection of Sensitive Compartmented Information;* DoDM 5200.01

Volume 1, *DoD Information Security Program: Overview, Classification, and Declassification;* DoDM 5200.01 Volume 2, *DoD Information Security Program: Marking of Information*; and DoDM 5200.01 Volume 3 *DoD Information Security Program: Protection of Classified Information*.

A1.10. Authority and responsibility relating to the management, administration, and oversight of the DAFSE, as delegated and assigned to the SecAF, pursuant to DoDD 5200.43, *Management of the Defense Security Enterprise*.

A1.11. Responsibility relating to DoD Controlled Unclassified Information Program, as delegated to the SecAF, pursuant to DoDI 5200.48, *Controlled Unclassified Information (CUI)*.

A1.12. Responsibility relating to SAP policy, as delegated to the SecAF, pursuant to DoDD 5205.07.

A1.13. Authority relating to the management, administration, and oversight of DoD SAPs, as delegated to the SecAF, pursuant to DoDI 5205.11.

A1.14. Authority and responsibility relating to policy, oversight, and implementation of the DAF C-InTP, as delegated to the SecAF, pursuant to DoDD 5205.16, *The DoD Insider Threat Program*, Administrative Instruction 121, *OSD Insider Threat Program* and assigned responsibility from Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information* and Presidential Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*.

A1.15. Authority and responsibility relating to establishing user activity monitoring capabilities to protect national security systems, national security information, and to detect suspicious or anomalous activity indicative of potential insider threats pursuant to assigned responsibility from Presidential Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs,* and Committee on National Security Systems Directive No. 504, *Directive on Protecting National Security Systems from Insider Threat*.

A1.16. Responsibility relating to unauthorized disclosure of classified information to the public, as delegated to the SecAF, pursuant to DoDD 5210.50, *Management of Serious Security Incidents Involving Classified Information*, with the exception that the HICEs for the Air Force and Space Force retain responsibility for reporting unauthorized disclosure of classified information with regard to intelligence and intelligence-related information or personnel pursuant to EO 12333, DoDD 5210.50, and Intelligence Community Directive 701, *Unauthorized Disclosure of Classified National Security Information*.

A1.17. Responsibility relating to personnel investigations of DoD personnel at U.S. missions abroad, as delegated to the SecAF, pursuant to DoDI 5210.84, *Security of DoD Personnel at U.S. Missions Abroad*.

A1.18. Responsibility relating to DoD Presidential Support program, to include adjudication of DAF YANKEE WHITE nominations (but not DAF security investigations) for Presidential Support duties, as delegated to the SecAF, pursuant to DoDD 5210.55, *Department of Defense Presidential Support Program*.

A1.19. Authority relating to selection of DAF military and civilian personnel and contractor employees for assignment to presidential support activities, as delegated to SecAF, pursuant to

DoDI 5210.87, *Selection of DoD Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities (PSAs).* This authority may not be re-delegated.

A1.20. Responsibilities for the screening, nomination and continued evaluation of DoD military and civilian personnel and contractor employees assigned to, or utilized in, presidential support activities, pursuant to DoDI 5210.87, *Selection of DoD Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities (PSAs)*.

A1.21. Responsibility relating to National Industrial Security Program, as delegated to the SecAF, pursuant to DoDI 5220.31, *National Industrial Security Program,* DoDM 5220.32 V1, *National Industrial Security Program: Industrial Security Procedures for Government Activities,* and DoDM 5220.32 V2, *National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence (FOCI)*.

A1.22. Responsibility relating to Defense Industrial Personnel Security Clearance Review Program, as delegated to the SecAF, pursuant to DoDD 5220.6, *Defense Industrial Personnel Security Clearance Review Program*.

A1.23. Authority and responsibility relating to classified national security information responsibilities pursuant to Section 5.4 (d) of Executive Order 13526, *Classified National Security Information,* as the Senior Agency Official pursuant to Executive Order 13526 and DoDM 5230.30, *DoD Mandatory Declassification Review (MDR) Program,* with the exception that the HICEs of the Air Force and Space Force retain authority for intelligence and intelligence-related information pursuant to EO 12333 and Intelligence Community Directive 703, *Protection of Classified National Intelligence Including Sensitive Compartmented Information*.

A1.24. Authority and responsibility for the oversight of OUSD(I&S)-designated organizations, programs, and activities, which the SecAF has agreed to manage and administer and provide guidance, direction and resourcing for DAF specific initiatives and activities, pursuant to the Memorandum of Agreement Between the Office of The Under Secretary of Defense for Intelligence & Security (OUSD (I&S)) and the SecAF concerning the *Responsibilities and Functions for Under Secretary of Defense for Intelligence and Security (USD(I&S)-Designated Organizations, Programs, and Activities* (CDM 0010-21), 25 March 2021.

A1.25. Responsibility relating to the Enhanced Security Program to Support the DoD Innovation Initiative, as delegated to the Senior Agency Official for Security, pursuant to DoDI 5205.85, *Enhanced Security Program to Support the DoD Innovation Initiative*.

A1.26. Authority and responsibility for executing roles and responsibilities regarding operating, sustaining, and modernizing MPE capabilities on behalf of the SecAF pursuant to DoDD 5101.22E.

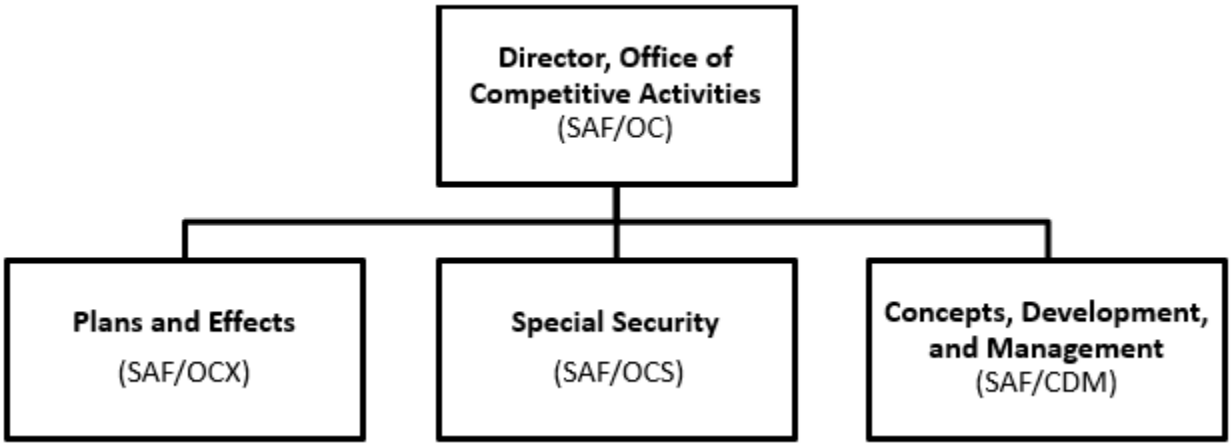
A1.27. Appointment authority for processing of official personnel actions on behalf of the SecAF pursuant to DAFPD 36-1, *Appropriated Funds Civilian Management and Administration* for all non-executive positions within the DAF Sensitive Activities Enterprise. All other civilian personnel authorities are delegated to SAF/MR pursuant to Headquarters Mission Directive (HAFMD) 1-24, *Assistant Secretary of the Air Force (Manpower and Reserve Affairs)*.

A1.28. Responsibility relating to providing prompt responses to Defense Counterintelligence and Security Agency personnel security lead requests from overseas military investigative agencies as delegated to the SecAF pursuant to DoDD 5105.42, *Defense Security Service (DSS)*.

A1.29. Responsibility to report all DoD intelligence and intelligence-related activities, to include sensitive activities, to the AF/A2 and SF/S2 for oversight, or when exceptions to policy are required, in accordance with DoDD 5148.13, *Intelligence Oversight* and DoDM 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, implemented by AFPD 14-4, *Management of the Air Force Intelligence, Surveillance, Reconnaissance, and Cyber Effects Operations Enterprise*.

Attachment 2

DIRECTOR, OFFICE OF COMPETITIVE ACTIVITIES (SAF/OC)



A2.1. Office of Competitive Activities (SAF/OC). The SAF/OC has overall responsibility, for the DAF, managing the security enterprise to include information, personnel, industrial security, counter insider threat program and the presidential support program; performing the roles and responsibilities of the DAF SAPCO; managing policy, oversight and integration of all competitive activities; managing and preparing policies for DAF sensitive activities; and managing and overseeing programs and activities as identified and directed by the SecAF to include assumption of roles and responsibilities assigned to the SecAF. The SecAF retains ultimate responsibility for all policies related to the DAF. Within their areas of responsibility, the SAF/OC develops and approves policies and programs, issues official guidance via Department level publications, and oversees the implementation and execution of those policies and programs.

A2.2. 3-Letter subordinate offices include:

A2.2.1. *Plans and Effects (OCX).* This Directorate's mission is to lead the assessments, planning, facilitation, and oversight, of the campaign activity plans that underpin the DAF's competitive activities portfolio while providing oversight, integration, synchronization and coordination of DAF sensitive activities as directed by SecAF. This includes requirements, opportunity identification, operational integration, and top-level relationships for a portfolio of activities that serve to further the competition goals of the DAF. This cross-functional team will incorporate functional experts in market analysis, intelligence, counterintelligence, acquisition, research, air and space operations, resources and public affairs, to conduct on-going assessments and identify asymmetries in warfighting concepts, capabilities and force design to exploit through influence activities and inform acquisition decisions and interdepartmental and interagency policy. SAF/OCX is also responsible for oversight of the DAF Special Program Assignments process, executed by the Air Force Personnel Center (AFPC), which assigns Airmen and Guardians to select positions within Special Programs and/or Sensitive Activities. The Directorate conducts triennial revalidations for Special Program Assignments support and promulgates SAF/OC's directed manning prioritization guidance for DAF personnel assigned to DAF, DoD, and non-DoD Federal Departments and Agencies-sensitive activities via AFPC. As tasked by SAF/OC and executed through a Concept

of Operations (CONOP) signed by former AAH Director and AF/A1, SAF/OCX will provide Commanders and Directors across the DAF with tailored classification and staffing support through its Civilian Sensitive Support Activity to ensure a qualified pool of civilians exists for DAF sensitive positions. SAF/OCX will work closely with Program Assessment and Evaluation (PA&E), Integrated Capabilities Office (ICO), Director for Air Force Studies and Analysis (SAF/SA) and other DAF organizations to ensure analyses completed by others are integrated and serve as a common baseline across the DAF corporate process.

A2.2.2. *Special Security (OCS).* The Special Security Directorate (SAF/OCS) administers and oversees policy for information security and the DAF Security Enterprise. SAF/OCS provides policy and oversight and management of the DAF C-InTP, Presidential Support Program, CUI, and Information, Industrial, and Personnel Security programs, which includes continuous vetting. SAF/OCS manages the execution of counter insider threat Hub operations. SAF/OCS also serves as the DAF SAPCO, as defined in DoDD 5205.07 and DoDI 5205.11. As the DAF SAPCO, the SAF/OCS is the principal advisor to SAF/OC, SecAF, and USecAF on SAP matters, provides policy, oversight and develops standards to ensure SAP security program core compliance, reducing risk of compromise of SAP information. SAF/OCS supports and coordinates with DoD SAPCO regarding SAP security matters and policy, to include SAP matters involving foreign governments. SAF/OCS provides strategic policy focus on the DAFSE and protection of information across the DAF. Responsible for convergence, integration, and information sharing of security activities across the DAFSE. SAF/OCS also executes responsibilities assigned to the Senior Agency Official for Security, as defined in DoDI 5205.85. SAF/OCS is also responsible for DAF declassification activities through the Department of the Air Force Declassification Office (DAFDO). DAFDO is responsible for developing declassification policy, guidance, and authorizing the continued protection of classified material past the 25-year mark for DAF classified equities. This includes executing declassification authority on behalf of the SAO, as outlined in DoDM 5200.01V1, in the performance of various declassification activities to include Automatic, Systematic, Mandatory, and Discretionary Reviews. DAFDO is responsible for all education, training, and awareness at the Department of the Air Force for historical declassification.

A2.2.3. *Concepts, Development, and Management (CDM).* This Directorate will support sensitive and competitive activities through designated requirements and agreements between DAF and other DoD and US government organizations, the interagency, and allies (e.g. OSD, CCMDs, Services, DoD Components, FVEYs, NATO.) SAF/CDM explores new concepts, cultivates emerging opportunities, develops capabilities, and manages high-priority projects and programs to provide innovative solutions to DAF and Defense-wide challenges, intelligence, and sensitive activities. SAF/CDM provides for the incubation, administration, management, and execution of designated programs and activities. Responsibilities include: working with partnering entities to identify problems; managing resources, cost, schedule, and performance of programs and activities; monitoring the objectives, functions, activities, and execution of tasks, taking action as required to facilitate successful execution and mission accomplishment; identifying program redundancies and recommending efficiencies through collaboration and synchronization of activities; engaging and coordinating, reporting, and maintaining appropriate dialogue with activity stakeholders and strategic partners on assigned tasks. SAF/CDM executes roles and responsibilities to deliver and sustain various enterprise capabilities. Pursuant to DoDD 5101.22E, in support of individual program sponsors and

coordination with the offices executing the duties of the DoD MPE EA, SAF/CDM manages resources, cost, schedule, and performance of DoD Enterprise MPE capabilities, programs and activities; acts as required to facilitate successful execution and mission accomplishment; and coordinates, reports, and engages with stakeholders and strategic partners.

Attachment 3

STANDARD OPERATING PROCEDURES FOR THE DIRECTOR, SECRETARY OF THE AIR FORCE, CHIEF INFORMATION OFFICER (SAF/CN), DIRECTOR, SECRETARY OF THE AIR FORCE, COMPETITIVE ACTIVITIES (SAF/OC)

A3.1 Purpose/Scope. This standard operating procedure (SOP) applies to individuals assigned to The Director, Office of Competitive Activities who fulfill the role and responsibilities of the DAF Special Access Program (SAP) cognizant authority (CA) consistent with Department of Defense Directive (DoDD) 5205.07, DoD Special Access Program Policy, and DoD Instruction (DoDI) 5205.11, Management, Administration, and Oversight of DoD Special Access Programs (SAPs). Providing policy, direction, administration, oversight and implementation of DAF SAP. These procedures facilitate routine staff actions and functions and reduce duplication of effort between SAF/OC and SAF/CN staff roles while increasing operating effectiveness and efficiency for SAP IT.

A3.2 Authorities and Delegations. This SOP does not enact or change two-letter delegations of authority or organizational relationships as reflected in HAFMD 1-26, HAFMD 1-15.

A3.3. SAF/OC and SAF/CN Share Oversight Authority and Responsibility for:

A3.3.1 SAF/OC SAPCO: Oversees and maintains a dedicated cadre of cybersecurity professionals to administer and execute SAP security, audit, compliance and cybersecurity (Risk Management Framework) activities for assigned SAPs in support of SAF/CN's IT and cybersecurity policy oversight and governance for the DAF. Designates management and execution roles within the SAP organizational structure (i.e., MAJCOM/FLDCOM SAP Management Offices (SAPMO), OSI/PJ, etc.) and ensures implementation, compliance, and accountability for SAP IT activities via SAP Compliance Inspection process, development of SAP Special Emphasis Items (SEIs), and SAP IT system Assessment and Authorization activities. This role focuses on: Administration and application of overall SAP IT security activities; execution of SAP-enhanced Risk Management Framework (RMF) procedures; and assignment of SAP support activities to outside organizations (SAPMOs, OSI/PJ, etc.).

A3.3.2 SAF/CN (DAF CIO) sets formal memoranda establishing roles and responsibilities for DAF IT RMF oversight, management, and execution. These overarching directives define the broad vision and strategic direction of IT and cybersecurity in the DAF. The DAF CISO establishes and manages the governance and oversight for the DAF IT in terms of RMF and overall cybersecurity compliance. SAF/CN provides guidance and sets the RMF and cybersecurity baselines for the DAF and is responsible for the inclusion of SAP-specific cybersecurity enhancements, appoints and provides oversight for a SAP Senior Authorizing Official (AO) and Subordinate AOs to each mission area requiring SAP-integrated support. DAF CISO appoints and provides oversight and training plans for all Security Control Assessors (SCAs). Defines artifacts and requirements for staffing of High Risk & Very High Risk (HR & VHR) ATO packages to the DAF CIO.

A3.4 Roles and Responsibilities.

A3.4.1. SAF/OCS:

A3.4.1.1. Reviews and advises the DAF CIO on appointment of SAP Subordinate AOs and SCAs to each mission area requiring SAP-integrated support. Executes DAF CISO SCA training plans. Conducts artifact and requirement review of HR & VHR ATO packages for recommendation and staffing to the DAF CIO.

A3.4.1.2. Coordinate with DAF CIO Records Manager to ensure compliance with federal law and record retention reporting. Implement SAP-compliant storage, access control, and archival processes for SAP records. Coordinate with external organizations to facilitate secure processing and storage of SAP-related records. Operationalizing records management policies, ensuring secure storage, restricted access, and proper archival procedures of SAP records while maintaining compliance with DoD and DAF directives and federal law.

A3.4.1.3. Collects and submits reports, dashboards, and situational awareness updates in accordance with SAF/CN governance criteria.

A3.4.1.4. Designate management and execution roles within the SAP Enterprise organizational structure (i.e., SAPMOs, OSI/PJ, SAPs) and ensure implementation, compliance and accountability.

A3.4.1.5. In coordination with SAPMO Cybersecurity Teams and other external stakeholders, assesses risk, performs testing, and develops integration strategies aligned with SAP mission needs.

A3.4.1.6. Manages and conducts SAP IT cloud risk assessments, implementations, and ensures compliance with DAF cybersecurity mandates.

A3.4.1.7. In coordination with SAPMOs populates cybersecurity scorecards and supports continuous improvement activities.

A3.4.1.8. In coordination with SAPMOs, track, report, and analyze metrics in alignment with DOD and DAF governance requirements.

A3.4.1.9. Oversee and coordinate with SAP stakeholders all SAP IT risk discussions and ensure decisions are documented and communicated.

A3.4.1.10. Regarding cybersecurity supply chain risk management, establishes SAP enhanced guidance and restrictions for acquisition and procurement of IT and cybersecurity products.

A3.4.1.11. Coordinate reviews and updates with publishing authorities for cybersecurity publications and forms.

A3.4.1.12. Executes the role of Senior Authorizing Official for the SAP Enterprise and for IT designated as SAP Enterprise Networks.

A3.4.1.13. Reports to DAF CIO on DoD 8140, *Cyberspace Workforce Management* foundational qualification validation for the DAF SAP IT workforce.

A3.4.1.14. Ensures implementation and compliance with applicable Commercial Internet Service Provider (CISP) policy; to include the management and accountability of SAPs utilizing CISP.

A3.4.1.15. Plan, coordinate, and execute audits, address findings and track resolution.

A3.4.1.16. Ensure SAPs comply with IT portfolio management processes, procedures and reporting.

A3.4.1.17. Establishes mechanisms, processes, and procedures for inventory management, including the tracking, auditing, and maintenance of IT asset records for SAP specific infrastructure, systems, hardware, and software.

A3.4.1.18. In coordination with SAPMOs, contribute to data collection, reporting, and remediation planning for CIO risk assessments.

A3.4.1.19. Identifies, evaluates, and authorizes cybersecurity tools and enterprise capabilities for the SAP IT Enterprise and SAP Enterprise IT.

A3.4.1.20. Coordinates with SAF/CN to implement an organizational structure, process, and procedures for Ports, Protocols, and Services Management (PPSM). Ensures implementation and compliance for PPSM across SAP IT Enterprise.

A3.4.1.21. Inspect SAPs to ensure vulnerabilities are identified, tracked and remediated in accordance with SAP IT policy and organizational vulnerability management plans.

A3.4.1.22. Manage SAP Mission Partner Environment (MPE) access, sharing protocols, and enforce data protection with appropriate MPE stakeholders.

A3.4.1.23. Implements and ensures Zero Trust strategy is incorporated in the design of Enterprise IT capabilities, networks, and systems.

A3.4.1.24. Ensure Identity, Credentials, and Access Management (ICAM) solutions comply with SAP IT policies and are implemented in Enterprise IT capabilities, networks, and systems.

A3.4.1.25. Inform SAPMOs of COMSEC requirements and ensure compliance across the SAP IT Enterprise.

A3.4.1.26. Evaluates the Enterprise Security Architecture to ensure capabilities, networks, and systems comply with DOD and DAF cybersecurity standards.

A3.4.1.27. In coordination with the field offices submit, justify, and track exception requests for SAP systems exception to DoD and DAF policy.

A3.4.1.28. Manages and oversees the SAP Insider Threat Program by evaluating behavioral indicators, assess risks, and implement detection, response mechanisms and user activity monitoring (UAM) in coordination with the Insider Threat Hub.

A3.4.1.29. In coordination with SAPMOs oversee continuous monitoring of SAP IT systems and maintain dashboards and alerting mechanisms.

A3.4.1.30. Plan, execute, and report on red/pentest team engagements and cybersecurity exercises that are led by the SAPMOs.

A3.4.1.31. Implement procedures, conduct post-incident analysis, and update playbooks for Incident Response Management.

A3.4.1.32. Oversight of Defense Industrial Base (DIB) for sharing threat data, support incident response, and coordinate remediation with cleared contractors.

A3.4.1.33. Oversee the response to and documenting of spillage events, conduct cleanup, and implement corrective actions.

A3.4.1.34. Coordinates with SAPMOs and SAP stakeholders to develop and exercise COOP plans, maintain alternate site readiness, and lead restoration efforts.

A3.4.2. SAF/CN:

A3.4.2.1. Establishes governance over cyberspace operations relevant to SAP environments, including alignment with national defense objectives and DAF cybersecurity directives.

A3.4.2.2. Define guidance for DAF IT-related records retention, classification, and compliance with federal records mandates, ensuring alignment with DoD and DAF IT Enterprise standards. Ensures compliance with federal law and align with broader DAF and DoD standards for records retention and classification.

A3.4.2.3. Establishes SAP-specific cybersecurity reporting requirements for metrics, compliance, and risk posture.

A3.4.2.4. Set formal memoranda establishing roles, responsibilities, authorities, and accountability for SAP IT oversight, management, and execution.

A3.4.2.5. In coordination with DoD SAP CIO, establishes governance and oversight mechanisms for evaluating and approving emerging technologies for use within the DAF.

A3.4.2.6. Govern review cycles of program cybersecurity strategies to ensure SAP IT alignment with enterprise risk.

A3.4.2.7. Define cybersecurity expectations and compliance requirements for SAP IT acquisitions.

A3.4.2.8. In coordination with DoD CIO, establishes oversight for the use of commercial cloud services within the DAF and provides the cybersecurity for cloud baseline security controls.

A3.4.2.9. Establishes metrics for evaluating cybersecurity maturity across SAP programs.

A3.4.2.10. Define and prioritize cybersecurity metrics for SAP IT performance and compliance.

A3.4.2.11. Serves as the senior risk advisor for SAP IT cybersecurity decisions.

A3.4.2.12. Governs third-party and supply chain cybersecurity risk posture.

A3.4.2.13. Ensures SAP IT compliance with Clinger-Cohen Act (CCA) requirements related to IT investments.

A3.4.2.14. Oversee cybersecurity inputs to publications and official forms.

A3.4.2.15. Govern and establish RMF processes, and implementation across SAP IT Enterprise. Coordinates with SAF/OC SAPCO on High/Very High Risk ATOs.

A3.4.2.16. Collects and reports to DoD CIO on DoD 8140*, Cyberspace Workforce Management* foundational qualification validation for the DAF IT workforce.

A3.4.2.17. Establishes a guidance memorandum for the management of CISP connections.

A3.4.2.18. Oversee audit scope and frequency for SAP IT and RMF-related cybersecurity assessments.

A3.4.2.19. Establishes governance and guidance on SAP IT Portfolio Management, ensuring oversight and accountability of SAP IT assets and IT expenditures across the SAP IT Enterprise.

A3.4.2.20. Establishes guidance for SAP IT asset management.

A3.4.2.21. Define metrics and ratings to evaluate SAP cybersecurity performance under enterprise compliance frameworks.

A3.4.2.22. Establishes governance and standards for cybersecurity tools deployed across the SAP IT Enterprise. Evaluates and advocates for cybersecurity tools and enterprise capabilities for use and implementation across the SAP IT Enterprise and/or SAP Enterprise IT.

A3.4.2.23. Governs and establishes guidance for PPSM and network services across SAP IT Enterprise.

A3.4.2.24. Define vulnerability management coordination procedures for SAP environments.

A3.4.2.25. Establish governance over Cross Domain Solutions (CDS) use to ensure compliance with data protection standards.

A3.4.2.26. Define cybersecurity guidance for collaboration environments with mission partners.

A3.4.2.27. Sets guidance for managing privileged access and enforcing separation of duties.

A3.4.2.28. Promote security development practices and integration of security into CI/CD pipelines.

A3.4.2.29. Define how data is handled, protected, and utilized for security insights.

A3.4.2.30. Develop a Zero Trust Architecture (ZTA) strategy for SAP environments.

A3.4.2.31. Identity, Credentials, and Access Management (ICAM), Identity Management (IdM), Public Key Infrastructure (PKI); set guidance for digital identity, access control, and cryptographic trust.

A3.4.2.32. Governs the protection of SAP IT communications through cryptographic measures.

A3.4.2.33. Oversee enterprise security architecture standards across SAP IT enclaves.

A3.4.2.34. Set procedures for managing and adjudicating exceptions within SAP IT cybersecurity policies.

A3.4.2.35. Promote secure software development and resilient system design practices.

A3.4.2.36. Establish SAP-focused insider threat and UAM detection governance and coordinate with enterprise programs.

A3.4.2.37. Define Information Security Continuous Monitoring ISCM requirements tailored to SAP system risks and compliance goals.

A3.4.2.38. Designate and oversee Cybersecurity Service Provider (CSSPs) supporting SAP operations, ensuring they meet DAF and DoD standards to deliver monitoring, incident detection, and analysis services for SAP customers.

A3.4.2.39. Establish oversight for red team operations and independent cybersecurity assessments within SAP.

A3.4.2.40. Develop SAP-specific incident response governance in alignment with enterprise frameworks.

A3.4.2.41. Define coordination mechanisms between SAP cybersecurity leadership and DIB partners.

A3.4.2.42. Establish containment and reporting for classified data spills in SAP environments.

A3.4.2.43. Set governance for SAP IT disaster recovery and continuity programs.

A3.5 Revisions to Standard Operating Procedures. These operating procedures may be reviewed and revised as deemed necessary by the Secretary of the Air Force. SAF/OC or SAF/CN may also initiate a revision in consultation with the appropriate principals. OPRs must follow revision procedures as mandated in HOI 90-1.

A3.6 Terms of the Agreement. This agreement may be reviewed and revised as deemed necessary by the SECAF. This SOP is effective once both parties have signed and may only be terminated or amended upon agreement by SAF/CN and SAF/OC.

AGREED:

For SAF/CN—

JENNIFER M. OROZCO, SES, DAF
Acting Chief Information Officer
Office of the Secretary of Air Force
(SAF/CN)

For SAF/OC—

EDWIN H. OSHIBA, SES, DAF
Director, Competitive Activities
Office of the Secretary of the Air Force
(SAF/OC)

Attachment 4

STANDARD OPERATING PROCEDURES (SOPs) BETWEEN THE OFFICE OF COMPETITIVE ACTIVITIES (SAF/OC) AND PUBLIC AFFAIRS (SAF/PA)

A4.1. Purpose: Establish procedures to synchronize operations between the SAF/OC and SAF/PA to enable timely, accurate, and credible communication in support of Department of the Air Force (DAF) competitive activities. The following guidance and procedures are intended to facilitate and deconflict staff actions and functions while increasing operational effectiveness.

A4.1.1. Applicability: These SOPs apply to all SAF/OC and SAF/PA divisions, relevant MAJCOM/FLDCOM PA personnel, and cross-functional working groups engaged in support of competitive activities.

A4.1.2. Governance and Compliance: This SOP aligns with Department of Defense (DoD) Principles of Information, DAFI 35-101, AFMAN 35-101, and applicable classification, declassification, and release authorities. Revisions may be initiated by SAF/OC, SAF/PA, or directed by the Secretary of the Air Force (SecAF). The Department's handling of overt and public information will continue to adhere to the DoD Principles of Information with an emphasis on accuracy and credibility—to include negative information that the DAF is obligated to provide as a government institution.

A4.2. Roles and Responsibilities

A4.2.1. SAF/PA Responsibilities:

A4.2.1.1. Retains its authorities, as assigned in Headquarters Air Force Mission Directive 1-28 and other publications, including release of public information and its direct reporting relationship to the SecAF and Service Chiefs.

A4.2.1.2. Provide independent advice to senior leaders, as necessary.

A4.2.1.3. Lead command information, Operations Security (OPSEC) PA guidance, public release planning, and campaign synchronization for public communication activities.

A4.2.2. SAF/OC Responsibilities:

A4.2.2.1. Advise the SecAF on all matters pertaining to competitive activities strategic planning, assessments, and resourcing supporting enterprise competition priorities as well as informing enterprise-level decisions for the DAF.

A4.2.2.2. Provide policy, oversight, and guidance of competitive activities across the DAF, which include activities related to DAF Operations, Activities, and Investments (OAIs) that, by design, shift the focus of strategic competition into areas that favor DAF interests and functions.

A4.2.2.3. Lead the coordination and synchronization of DAF competitive activities.

A4.2.2.4. Develop policy and planning guidance to advance competitive posture and safeguard critical information.

A4.2.2.5. Ensures an adequate number of PAs at the SAF, MAJCOM and FLDCOM levels have the necessary clearances to be involved in effective cross-functional planning.

A4.2.2.5. Integrates PA tracking and metrics into OC planning frameworks.

A4.2.3. Shared Responsibilities:

A4.2.3.1. Coordinate cross-functional planning, assessments, and execution.

A4.2.3.2. Provide joint recommendations to senior leaders.

A4.2.3.3. Participate in relevant working groups (e.g., IWWG, ATWG).

A4.3. Organizational Coordination

A4.3.1. SAF/PA divisional support to SAF/OC

A4.3.1.1. SAF/PAX (Strategy and Assessments Division) serves as the SAF/PA representative for SAF/OC communication planning and assessments, supports efforts to provide a common operating picture of communication activities, and drafts supporting PA campaign goals, objectives, and execution plans.

A4.3.1.2. SAF/PAO (Media Operations Division) coordinates on short-term issues affecting the release of information on competitive activities and drafts supporting PA Guidance (statements/releases, questions, and answers).

A4.3.1.3. SAF/PAI (Command Information Division) and the Air Force Public Affairs Agency (AFPAA) coordinates on the use of web sites, social media platforms and visual information in support of competitive activities.

A4.3.1.4. SAF/PAY (Engagement Division) coordinates on the use of think tank engagements to execute, or red-team, communication in support of competitive activities.

A4.3.1.5. SAF/PAY and SAF/PAB (Bands Division) as appropriate coordinate on the use of civic outreach in support of competitive activities.

A4.3.1.6. SAF/PAR (Requirements Division), the SAF/PA Director of Staff and AFPAA, as appropriate, coordinates on resource or policy requirements linked to competitive activities.

A4.3.1.7. Security & Policy Review: SAF/OC will have the opportunity to provide input on publicly releasable products through SAF/PA's existing S&PR process.

A4.3.2. SAF/OC divisions support to SAF/PA

A4.3.2.1 SAF/OCX (Competition Plans and Effects) Leads assessments, planning, and oversight of campaign activity plans that underpin the DAF's competitive activities portfolio, while providing oversight, integration, synchronization, and coordination of DAF sensitive activities. SAF/OCX incorporates SAF/PA into planning efforts to ensure PA equities and issues are addressed.

A4.3.2.2 SAF/CDM (Concepts, Development, and Management) Explores new and enduring concepts, cultivates emerging opportunities, develops capabilities, and manages high-priority projects and programs to provide innovative solutions for DAF competitive activities requirements and defense-wide challenges within the intelligence, sensitive activities, and SAP portfolios. SAF/CDM coordinates with SAF/PA to ensure concepts and capabilities account for PA requirements and equities.

A4.3.2.3 SAF/OCS (Special Security) Enhances collateral security and DAF Special Access Program Central Office (SAPCO) functions by facilitating information sharing across highly restricted, classified channels to accelerate delivery of cross-functional mission sets for the U.S. defense apparatus. SAF/OCS ensures adequate SAF/PA access to programs to enable planning and prevent conflicting messaging.

A4.3.3. Rapid Coordination:

A4.3.3.1. For emerging issues with obvious SAF/OC equities, SAF/PA will coordinate with SAF/OC to ensure SAF/OC is informed of public communication activities and can provide timely input on strategic messaging or posture considerations.

A4.3.3.2. Existing or ad hoc liaison structures should be used for time-sensitive topics.

A4.3.3.3. SAF/OC and SAF/PA will coordinate as a Quick Reaction Force (QRF) on breaking matters where each serve as stakeholders to ensure desired outcomes regarding Quality Assurance, Security, and Perception Management.

A4.3.4. Deconfliction:

A4.3.4.1. SAF/PA and SAF/OC retain the right to present differing recommendations.

A4.3.4.1.1. The Director of Public Affairs, as the designated authority for the release of public information, reserves the right to provide independent advice to DAF leaders.

A4.3.4.1.2. The Director of the Office of Competitive Activities, who provides policy guidance in clandestine and sensitive operations in the competitive environment, reserves the right to provide independent advice to DAF leadership.

A4.3.4.2. In the event there are significant concerns regarding implementing guidance from the respective organizations, an attempt will be made at the lowest level to resolve the conflict to ensure execution. If not resolved, then it will go to the Director, SAF/OC and the Director, SAF/PA. If they cannot resolve the conflict, then it must be adjudicated by the Secretary or Under Secretary.

A4.4. Communication Integration Process: SAF/OC and SAF/PA should use existing or ad hoc cross-functional working groups or direct liaison with the agency responsible to ensure appropriate coordination.

A4.4.1. Planning:

A4.4.1.1. Designated SAF/OC personnel will serve as an interface and touchpoint for SAF/OC to align operations to achieve mission objectives.

A4.4.1.2. SAF/OC will proactively notify SAF/PA of known or anticipated developments in competitive activities that may generate media interest, public scrutiny, or require deliberate messaging coordination.

A4.4.1.3. SAF/PA will integrate into SAF/OC planning cycles, and vice versa, for competitive activities and contribute to the development of joint communication guidance.

A4.4.1.4. SAF/PA personnel and appropriate PA staff at field headquarters and units will be involved in cross-functional planning to the greatest extent possible under expanded classification compartments, which will include, but is not limited to, working directly with subject matter experts within Information Operations, Intelligence, and Special Investigation communities. PA expertise is essential not only for planning and executing public communication, but also for evaluating whether the observable footprints of advanced technology programs or operational activities will require PA safeguards or mitigation strategies.

A4.4.2. Execution: SAF/OC and SAF/PA will focus their collaboration primarily on overt communication in two areas of competitive activity: Air Force and Space Force *Operations* and *Investments*. This focus extends to activities, such as public releases, media and think tank engagements, or industry panels at conferences. This does not include activities where PA is not the lead communicator, such as congressional

testimony, budget documents and comptroller materials, contract RFIs, etc. Decision-making and execution on public communication activities will be delegated to the lowest reasonable level, consistent with this plan and applicable DoD and DAF directives and instructions.

A4.4.2.1. Operations:

A4.4.2.1.1. Communications on service component operations are often governed by Combatant Command (CCMD) guidance. SAF/OC and SAF/PA will seek additional guidance on these operations with prior CCMD coordination.

A4.4.2.1.2 SAF/PA will provide standing Operations Security (OPSEC) guidance for continuous service operations and coordinate regular updates for that guidance with SAF/OC.

A4.4.2.1.3 SAF/PA will provide ad hoc OPSEC guidance on emerging operations as required. In cases where the need for guidance outpaces formal staffing, SAF/PA will brief SAF/OC on current guidance and issue supplemental guidance as required.

A4.4.2.1.4. SAF/PA management of operations-related communication will be managed through SAF/PAX's Information Warfare Working Group (IWWG), which includes SAF/PA representatives across divisions actively engaged in influence planning at the MAJCOM/FLDCOM level and below. SAF/OC will have a standing invitation to the IWWG.

A4.4.2.2. Investments / Acquisitions:

A4.4.2.2.1. Major acquisition programs and associated operations (testing, fielding, sustainment) that require active oversight by the competitive enterprise will be identified and managed in accordance with processes outlined in the SAF/OC charter.

A4.4.2.2.2. SAF/PA will provide standing guidance for service advanced technology programs and coordinate regular updates to that guidance with SAF/OC.

A4.4.2.2.3. SAF/PA will provide ad hoc guidance on capability development or acquisition programs as required. In cases where the need for guidance outpaces formal staffing, SAF/PA will brief SAF/OC on current guidance and issue supplemental guidance as required.

A4.4.2.2.4. SAF/PA management of investment-related communication will be managed through SAF/PAX's Advanced Technology Working Group (ATWG), which includes SAF/PA representatives across divisions

actively engaged in influence planning at the MAJCOM/FLDCOM level and below. SAF/OC will have a standing invitation to the ATWG.

A4.4.3. Review and Assessments:

A4.4.3.1. SAF/PA and SAF/OC will coordinate to integrate engagement tracking and communication effectiveness metrics.

A4.4.3.2. SAF/OC will utilize existing PA enterprise systems for continuity and reduce redundant reporting unless otherwise agreed upon.

A4.4.3.3. SAF/PA and SAF/OC will share assessments of communication performance and effectiveness to inform future recommendations and decision-making.

A4.5. Revisions to Standard Operating Procedures: These operating procedures may be reviewed and revised as deemed necessary by the Secretary or Under Secretary of the Air Force. SAF/OC and SAF/PA may also initiate a revision.

AGREED:

For SAF/PA –

TIMOTHY A. HERRITAGE
Brigadier General, USAF
Director, Public Affairs
(SAF/PA)

For SAF/OC –

EDWIN H. OSHIBA, SES, DAF
Director, Competitive Activities
Office of the Secretary of the Air Force
(SAF/OC)