BY ORDER OF THE
SECRETARY OF THE AIR FORCE

HEADQUARTERS AIR FORCE
MISSION DIRECTIVE 1-26

14 JUNE 2023

CHIEF INFORMATION OFFICER

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Headquarters Air Force Publications and forms are available on the e-Publishing website at **http://www.e-publishing.af.mil**

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/CNZA

Certified by: Lauren Knausenberger

Supersedes: HAFMD 1-26, (February 5, 2015)
HAFMD 1-5, (September 13, 2019)

Pages: 16

This revision includes significant changes due to role, responsibility, and organizational adjustments to reflect the separation and realignment of the A6 on the Air Staff and Chief Information Officer (CIO) function on the Secretary of the Air Force staff, stand-up of the U.S. Space Force, and alignment of the Department of the Air Force (DAF) Chief Data and Artificial Intelligence Officer (CDAO) under the CIO in SAF/CN to address data and artificial intelligence (AI) policy and governance. It also incorporates changes in federal law and Department of Defense (DoD) directives and instructions; updates references that have been superseded, changed, realigned or rescinded.

1. Mission . The Secretary of the Air Force (SecAF), pursuant to Title 10 United States Code (USC) §§ 9014, may establish offices and officials within the Secretariat to assist the SecAF in carrying out his/her responsibilities. As documented by **Paragraph 4.1.7** of Air Force Mission Directive 1, *Headquarters Air Force*, and this Headquarters Air Force Mission Directive (HAFMD), the DAF Chief Information Officer (SAF/CN) is established as part of the Secretariat. The SAF/CN has responsibility for information technology, cybersecurity, enterprise data management (as defined in Department of the Air Force Instruction 90-7001, *Enterprise Data Sharing & Data Stewardship*, dated April 22, 2021), AI policy and governance, information management, and information resources management for the DAF. The portfolio includes oversight of unclassified, classified, and Special Access Programs (SAP) information technology not including those for Sensitive Compartmented Information (SCI) and other intel-funded capabilities regardless of classification level), in accordance with Title 40, Title 44, and OMB Circular authorities, in support of the Department of the Air Force. The Secretary retains ultimate responsibility for all policies related to the DAF. Within their areas of responsibility, the SAF/CN prepares policies for approval and issues official guidance via official DAF publications to ensure implementation of those policies.

2. Organizational Relationships . The SecAF is responsible for, and has all legal authority necessary to conduct, the affairs of the DAF. The Secretariat, the Chief of Staff of the Air Force (CSAF), the Chief of Space Operations (CSO), the Air Staff, and the Office of the Chief of Space Operations (informally known as the Space Staff) perform their DAF functions subject to the authority, direction, and control of the SecAF.

2.1. The SAF/CN reports to the SecAF, serves as an agent of the 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 his/her area of responsibility. The SAF/CN is accountable to the SecAF for results achieved within the policy and program domains assigned by this directive.

2.2. The SAF/CN is a member of the Secretariat and as such works closely with other Headquarters Air Force (HAF) offices to assist the SecAF in carrying out his/her responsibilities. The SAF/CN and the Office of the SAF/CN work in cooperation with the CSAF, CSO, Vice Chief of Staff of the Air Force (VCSAF), Vice Chief of Space Operations (VCSO), the Under Secretary of the Air Force (USecAF), the Assistant Secretaries of the Air Force and their respective offices, as well as other HAF organizations, which are responsible, pursuant to Chapters **903**, **905**, **907**, and **908** of Title 10 (10 USC §§ 9011-9024, §§ 9031-9040, and §§ 9081-9084), for assisting the SecAF in carrying out his/her responsibilities.

2.2.1. Pursuant to Headquarters Operating Instruction 90-1, *Headquarters Air Force Mission Directives and Department of Defense Issuances Program*, two or more HAF two-letter/digit organizations with responsibilities in the same functional area are encouraged to develop standard operating procedures (SOP) that set forth procedures enabling covered organizations to fulfill and carry out their respective missions, roles, and responsibilities. As of the date of this publication, SAF/CN is not a party to any SOPs; however, recognizing major recent changes to the Department, SAF/CN will explore SOPs with Secretariat, Air and Space staff organizations and add to the MD, as finalized.

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

3.1. Advising the SecAF on all matters pertaining to information technology strategic planning, transformation, and modernization.

3.2. Overseeing DAF information technology digital transformation and cybersecurity.

3.3. Focusing predominantly on systems, connections, processes, and policies across the DAF at the enterprise level.

3.4. Working in close coordination with the DAF Principal Cyber Advisor to ensure Air Force and Space Force are aligned with the Department of Defense Cyber Strategy.

3.5. Liaising with DoD and other Military Department CIOs.

3.6. Coordinating with the Joint Staff with respect to information technology and national security systems (NSS) (as defined in 40 USC § 11103(a)(1)).

3.7. Driving a culture of digital technology adoption and innovation for DAF civilian and military employees.

3.8. In concert with the human capital senior leaders, enhancing information technology and digital technical fluency across the DAF work force.

3.9. Overseeing provision and continual improvement of foundational levels of the information technology hardware and software infrastructure and driving innovation of the same.

3.10. Establishing and overseeing information technology change management processes and procedures.

3.11. Providing advice and other assistance to DAF executive leadership on acquisition and management of information technology.

3.12. Assisting the SecAF in carrying out responsibilities for information management and information resources management to improve DAF productivity, efficiency, and effectiveness.

3.13. Setting and ensuring DAF compliance with government-wide and DoD enterprise information technology policies, principles, standards, and guidelines, and representing the DAF on the DoD CIO Joint Enterprise Standards Committee.

3.14. Assuming responsibility and accountability for DAF information technology investment management.

3.14.1. Reviewing budget requests for all DAF information technology and NSS.

3.14.2. Monitoring and evaluating the performance of information technology programs and advising the SecAF whether to continue, modify or terminate a program or project.

3.14.3. Issuing guidance to provide for the coordination of, and decision-making for, the planning, programming, and control of investments in information technology portfolio management.

3.14.4. Establishing and leading DAF information technology governance councils, boards, and groups.

3.15. Developing DAF Information Environment Architecture for data and systems.

3.16. Serving as the DAF Interoperability Lead for information technology and NSS and as the DAF representative to the DoD CIO Interoperability Steering Group.

3.17. Designating a Chief Information Security Officer (CISO) to perform cybersecurity duties for the DAF.

3.17.1. Ensuring cybersecurity and risk management of systems and platform information technology (also known as operational technology).

3.17.2. Recommending DAF Authorizing Officials for all DAF information systems and platform information technology (also known as operational technology) for DAF CIO appointment.

3.18. Operating as the Functional Authority for the DAF Communications and Information/Cyber civilian career field providing oversight for overall talent management including force renewal, force development, and force management.

3.19. Tracking and ensuring DAF compliance with information resources management requirements, public laws and higher-echelon publications and policies.

3.19.1. Designating a Chief Freedom of Information Act (FOIA) Public Liaison Officer and issuing FOIA policy for the DAF.

3.19.2. Appointing a DAF Senior Component Official for Privacy (SCOP) and issuing Department privacy and civil liberties policy.

3.19.3. Designating a DAF Senior Agency Official for Records Management.

3.19.4. Overseeing the collection and quality of information within the DAF and the control of the paperwork burden.

3.19.5. Establishing and maintaining a DAF information technology accessibility program to ensure electronic and information technology are developed, procured, and maintained to provide access to the disabled, to the maximum extent practicable.

3.19.6. Issuing Knowledge Management policy to enable all DAF organizations to effectively and efficiently leverage knowledge as a strategic resource and maintain the life cycle of information.

3.19.7. Appointing a Federal Register Liaison Officer and issuing policy on the DAF Federal Register Program process.

3.19.8. Ensuring DAF compliance with information technology-related requirements of the Clinger-Cohen Act of 1996 (40 USC §§ 11101-11704).

3.20. Overseeing and managing SAP enterprise information technology governance, standards, interoperability, and cybersecurity and serving as a member of appropriate oversight and governance bodies.

3.21. Leading DAF cryptographic modernization and key management efforts, including leading DAF input and recommendations to the Military Command, Control, Communications and Computers (C4) Executive Board (MC4EB) process.

3.22. Overseeing measurement of DAF information technology service quality and service management capability and submitting associated reports to enable an enterprise view on the delivery efficiency of information technology services' ability to meet DoD mission and business enterprise requirements.

3.23. Overseeing and resourcing the DAF CDAO and supporting office who are responsible for the advancement and operationalization of data and AI across the DAF enterprise. Specific CDAO responsibilities include:

3.23.1. Enterprise lifecycle data management to ensure the data needs of the Department of the Air Force are met, to include coordinating with any official in the DAF on the use, protection, dissemination, and generation of data.

3.23.2. Leading DAF AI and Responsible Artificial Intelligence (RAI) policy, governance, and implementation.

3.23.3. To the extent practicable: ensuring the DAF maximizes the use of data for strategic advantage, including for the production of evidence (as defined in 44 USC § 3561), cybersecurity, and the improvement of DAF operations; ensuring DAF data conforms to data management best practices; and encouraging collaborative approaches on improving data use.

3.23.4. Carrying out the requirements of the DAF under 44 USC § 3511 by developing and maintaining a comprehensive inventory of all DAF data assets created by, collected by, under the control or direction of, or maintained by the DAF.

3.23.5. Preparing data policy, and issuing guidance, and procedures for the management of DAF data assets at all classification levels (excluding SCI and other intelligence data), including the standardization of data format, sharing of data assets, and publication of data assets.

3.23.6. Reviewing the impact of the infrastructure of the DAF on data asset accessibility to make recommendations on required infrastructure improvements to reduce barriers that inhibit data asset accessibility. Submitting compliance reports as required by statute or policy.

3.23.7. Consistent with DoDI 8320.07, *Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense*, identifying data and AI capabilities and aligning them with Department of the Air Force and DoD strategies to develop data-centric investment strategies and to find solutions for areas of concern.

3.23.8. Plan, program, budget, and execute funding for enterprise-wide DAF capabilities that share data, AI, and information, and their supporting infrastructures to support data, AI, information, and information technology sharing capabilities.

3.23.9. Enhancing development of data science and data management skills across the Total Force to shape a data-driven DAF culture.

3.23.10. Establishing DAF-wide data and AI governance (policies, processes, practices, principles, and roles and responsibilities) and sponsoring DAF data and AI governance fora.

3.23.11. Providing direction, guidance, and oversight for data management operations across the DAF enterprise.

3.23.11.1. Implementing plans, processes, and procedures to ensure authoritative (trustworthy), actionable (current and relevant), assured (accurate and secured), and available (visible, accessible, and secured) data is captured, commonly available and represented (linked and interoperable) consistent with 44 USC § 3506(b) – (d), (f), and (i); 44 USC §3507, and Department of the Air Force policy, as well as aligned with SecAF, CSAF, and CSO communication strategies and plans.

3.23.11.2. Advising the SecAF, USecAF, CSAF, and CSO on opportunities to improve the use of and encourage collaborative approaches on data acquisition and use.

3.23.11.3. Cataloguing and publishing Open, Public, Electronic, and Necessary (OPEN) data in a standardized, non-proprietary format consistent with 44 USC § 3506.

3.23.11.4. Identifying points of contact for roles and responsibilities related to OPEN data use and implementation.

3.23.11.5. Engaging with agency employees, the public, and contractors in using public data assets, and encouraging collaborative approaches on improving data use.

3.23.11.6. Collaborating and supporting the Deputy Under Secretary of the Air Force, Management and Deputy Chief Management Officer, Office of the Under Secretary of the Air Force (SAF/MG) and the Director for Studies and Analysis, Office of the Secretary of the Air Force (SAF/SA) with the provision of data to carry out their respective roles in strategic and performance planning measurement and assessment, as well as analysis.

3.23.11.7. Serving as DAF standing member for DoD Chief Digital and AI Council and DAF liaison to other agencies and the Office of Management and Budget on best ways to use agency data for statistical purposes.

3.24. Coordinating with SAF/AQ and SAF/SQ on matters pertaining to acquisition of systems and services acquisition.

3.25. Functioning as the Category Manager for Category 1.0, Information Technology, with the full authority and responsibility to deliberately and proactively manage strategic costs in the category across the DAF.

4. Delegations of Authority/Assignment of Responsibility : **Attachment 1** lists delegated authorities and assigned responsibilities to the SAF/CN. The authorities delegated/responsibilities assigned to the SAF/CN by this Headquarters Air Force Mission Directive may generally be re-delegated unless re-delegation is expressly prohibited by the attached delegation or superseding law, regulation, or Department of Defense issuance. While the SAF/CN may re-delegate authorities to other DAF officials, he/she will ultimately be responsible to the SecAF for all matters listed in **Paragraph 1** of this publication. Any re-delegation of authority/assignment of responsibility made shall not be effective unless it is in writing. The re-delegation may be done as an addendum signed by the SAF/CN to this HAFMD. Any person re-delegating authority in accordance with this HAFMD may further restrict or condition the authority being re-delegated.

5. Notifications to Congress : No re-delegation of authority/assignment of responsibility under this HAFMD 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 publication remain effective insofar as such re-delegations are not inconsistent with the terms of this HAFMD unless superseded by a new re-delegation or assignment.

Frank Kendall
Secretary of the Air Force

ATTACHMENT 1

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

TO THE

CHIEF INFORMATION OFFICER (SAF/CN)

A1.1. Authority to maintain an inventory of all computer equipment under the control of the DAF that is excess or surplus property, as assigned to the SecAF pursuant to 40 USC § 11701.

A1.2. Authority, upon determining that the purpose of an information technology system is to disseminate information to the public, to reasonably ensure that an index of information disseminated by the system is included in the directory of Federal electronic information, as assigned to the SecAF pursuant to 40 USC § 11702.

A1.3. Authority to develop and maintain a comprehensive data inventory that accounts for all data assets created by, collected by, controlled by, directed by, or maintained by the DAF, and related responsibilities, as assigned to the SecAF pursuant to 44 USC § 3511.

A1.4. Authority to designate a DAF senior information security officer, as assigned to the SecAF pursuant to 44 USC § 3554.

A1.5. Authority for conducting periodic reviews of Social Security number use and reporting, as delegated to the SecAF pursuant to DoDI 1000.30, *Reduction of Social Security Number (SSN) Use Within DoD.*

A1.6. Authority for oversight of funding, managing, developing, operating, maintaining, evaluating, and improving DoD C2 information technology and NSS enabling capabilities, as delegated to the SecAF pursuant to DoDD 3700.01, *DoD Command and Control (C2) Enabling Capabilities.*

A1.7. Authority for operating telecommunications systems within the National Capital Region to support operational requirements, as delegated to the SecAF pursuant to DoDI 4640.07, *Telecommunications Services in the National Capital Region (NCR).*

A1.8. Authority for ensuring all airborne systems that transmit still and motion imagery and unmanned aircraft control communications systems comply with DoD guidance, as delegated to the SecAF pursuant to DoDI S-4660.04, *(U) Encryption of Imagery Transmitted by Airborne Systems and Unmanned Aircraft Control Communications* (Classified).

A1.9. Authority for establishing, sufficiently. resourcing, and maintaining the DAF records management program, to include designating an individual to serve as the DAF Senior Agency Official for Records Management and issue records management policy for the Department of the Air Force, as delegated to the SecAF pursuant to DoDI 5015.02, *DoD Records Management Program.*

A1.10. Authority for providing appropriate representation to governance bodies, as delegated to the SecAF pursuant to DoDI S-5100.92, *(U) Defense and National Leadership Command Capability (DNLCC) Governance* (Classified).

A1.11. Authority as DoD Component Lead for DAF Mission Partner Environment (MPE) actions pertaining to DAF responsibilities for IT and National Security System policy, interoperability, and investments. Coordinates with Air Force Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance (AF A2/6) and Space Force Chief Technology & Innovation Officer (SF/CTIO), as service leads for implementation of unique MPE capabilities supporting coalition information sharing. Coordinates with the DoD Executive Agent for DoD MPE, pursuant to DoDD 5101.22E, *DoD Executive Agent (DoD EA) for DoD Mission Partner Environment (MPE)*.

A1.12. Authority as DoD Component Lead for DAF MPE implementation pertaining to DAF responsibilities for IT and National Security System policy, interoperability, and investments. Coordinates with AF A2/6 and SF/CTIO, as service leads for their implementation of unique MPE capabilities to support unified actions across the full range of military operations. Responsibility for DoD Component-level implementation of an MPE and MPE capabilities to support unified actions across the full range of military operations, as delegated to the SecAF pursuant to *DoDI 8110.01, Mission Partner Environment Information Sharing Capability Implementation for the DoD*.

A1.13. Authority for advising and coordinating with the Defense Information Systems Agency, as delegated to the SecAF pursuant to DoDD 5105.19, *Defense Information Systems Agency (DISA).*

A1.14. Authority for coordinating with the Office of the DoD CIO on matters relating to the DAF information enterprise, as delegated to the SecAF pursuant to DoDD 5144.02, *DoD Chief Information Officer (DoD CIO).*

A1.15. Authority for ensuring compliance in Nuclear Command and Control programs, as delegated to the SecAF pursuant to DoDI S-5200.16, *(U) Objectives and Minimum Standards for Communications Security (COMSEC) Measures U3.sed in Nuclear Command and Control (NC2) Communications* (Classified).

A1.16. Authority for carrying out and administering a classified cryptographic information access program, in coordination with the Service Cryptologic Components, as delegated to the SecAF pursuant to DoDI 5205.08, *Access to U.S. Classified Cryptographic Information*.

A1.17. Authority for developing procedures and conducting cyber intrusion damage assessments in support of Defense Industrial Base Cybersecurity/Information Assurance (IA) activities; planning, programming, resourcing, and budgeting for costs associated with implementing policy; ensuring acquisition programs support Defense Industrial Base cybersecurity and IA activities, as delegated to SecAF pursuant to DoDI 5205.13, *Defense Industrial Base (DIB) Cybersecurity (CS) Activities*.

A1.18. Authority for obtaining document services through the Defense Logistics Agency (DLA), as delegated to the SecAF pursuant to DoDI 5330.03, *Single Manager of DoD Document Services.*

A1.19. Authority for administering the DAF FOIA Program, publishing related policy, conducting training for officials and employees who implement the FOIA program, as delegated to SecAF pursuant to DoDD 5400.07, *DoD Freedom of Information Act (FOIA) Program*.

A1.20. Authority for establishing the DAF Civil Liberties Program, providing adequate funding, and oversight in support of an effective DoD Privacy Program, to include the appointment of a senior official to serve as the DAF SCOP, as delegated to the SecAF pursuant to DoDI 5400.11, *DoD Privacy and Civil Liberties Programs.*

A1.21. Authority for establishing DAF policies and procedures to ensure compliance with DoD Privacy Act Assessment guidance and policies, as delegated to SecAF pursuant to DoDI 5400.16, *DoD Privacy Impact Assessment (PIA) Guidance*.

A1.22. Authority for overseeing and supporting the use of DAF capability portfolio management in order to advise senior leadership on capability investment and participating in capability portfolio forums, as delegated to the SecAF pursuant to DoDD 7045.20, *Capability Portfolio Management*.

A1.23. Authority for DAF information resources management (IRM) activities, creation of an information advantage for DAF personnel and mission partners, and information sharing between the DAF and mission partners, as delegated to the SecAF pursuant to DoDD 8000.01, *Management of The Department of Defense Information Enterprise (DoD IE)*.

A1.24. Authority for DoD Information Network (DODIN) transport and the life-cycle management of connection and interconnection of information systems, Unified Capabilities (UC) products, and access to information services, as delegated to SecAF pursuant to DoDI 8010.01, *Department of Defense Information Network (DODIN) Transport*.

A1.25. Authority for directing the development and use of a Knowledge Management process to promote sharing wireless technology capabilities, vulnerabilities, and vulnerability mitigation strategies, as delegated to SecAF pursuant to DoDD 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)*.

A1.26. Authority for planning, investment, development, operations, and management of DAF networks to support DoD UC policies, as delegated to the SecAF pursuant to DoDI 8100.04, *DoD Unified Capabilities (UC)*.

A1.27. Authority for managing DAF information technology investments as portfolios that focus on improving DoD capabilities and mission outcomes, as delegated to the SecAF pursuant to DoDD 8115.01, *Information Technology Portfolio Management*.

A1.28. Authority for overseeing implementation of DAF IT portfolio processes, as delegated to the SecAF pursuant to DoDI 8115.02, *Information Technology Portfolio Management Implementation*.

A1.29. Authority for providing DAF-specific cybersecurity orientation, training, awareness, and reinforcement programs to authorized users of systems as delegated to SecAF, pursuant to DoDD 8140.01, *Cyberspace Workforce Management*.

A1.30. Authority for overseeing the identification, tracking, data collection, and reporting requirements of DoD Cyberspace Workforce Framework (DCWG) work roles within the DAF, in coordination with human capital senior leaders, as delegated to the SecAF pursuant to DoDI 8140.02, *Identification, Tracking, and Reporting of Cyberspace Workforce Requirements*.

A1.31. Authority for establishing risk assessment procedures to evaluate and monitor DAF use of current and emerging information technologies, as delegated to SecAF pursuant to DoDI 8170.01, *Online Information Management and Electronic Messaging*.

A1.32. Authority for developing standardized enterprise force structure data, available electronically in a joint hierarchical way for integration and use throughout the DoD, to achieve the net-centric vision of Strategic Planning Guidance, as delegated to the SecAF pursuant to DoDI 8260.03, *The Global Force Management Data Initiative (GFM DI)*.

A**1.33.** Authority for ensuring information technology and NSS are compliant with U.S. Government and DoD standards requiring program managers for IT acquisitions and procurements to include standards compliant with DoD Architecture Framework, as delegated to SecAF pursuant to DoDI 8310.01, *Information Technology Standards in the DoD.*

A1.34. Authority for implementing policies and procedures to protect data, information, and information technology services across the DoD security domains with the intelligence community and mission partners, as delegated to SecAF pursuant to DoDI 8320.02, *Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense.* Note: AF A2/6 and SF/COO(S2) are responsible to the DNI for the protection of SCI and other intelligence data, information, and information technology services).

A1.35. Authority for enabling a secure sharing environment in the DAF that supports the warfighting, business, DoD intelligence, and enterprise information environment mission areas, as delegated to the SecAF pursuant to DoDI 8320.07, *Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense*.

A1.36. Authority for certifying interoperability of DAF information technology and NSS, as delegated to the SecAF pursuant to DoDI 8330.01, *Interoperability of Information Technology (IT), Including National Security Systems (NSS)*.

A1.37. Authority for ensuring accessibility of information and communication technology, to include designating an individual to serve as the DAF Section 508 Coordinator, as delegated to the SecAF pursuant to DoDM 8400.01, *Accessibility of Information and Communication Technology (ICT).*

A1.38. Authority for requiring the use of ".mil" as the primary top-level domain and ensuring accomplishment of DoD Component CIO-assigned tasks, as delegated to SecAF pursuant to DoDI 8410.01, *Internet Domain Name and Internet Protocol Address Space Use and Approval*.

A1.39. Authority for executing network management within the DAF Information Environment, as delegated to SecAF pursuant to DoDI 8410.03, *Network Management (NM)*.

A1.40. Authority for ensuring commercial wireless local-area network devices, systems, and technologies comply with DoD policy, as delegated to SecAF pursuant to DoDI 8420.01, *Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies*.

A1.41. Authority for providing input to and participating with DoD CIO in the collaborative development and annual review update of the DoD Enterprise Service Management Framework (DESMF), measuring information technology service quality and service management capability at a minimum annually or as additionally promulgated by the DoD CIO to enable an enterprise view on the delivery efficiency of information technology services ability to meet DoD mission

and business enterprise requirements, as delegated to SecAF pursuant to DoDI 8440.01, *DoD Information Technology (IT) Service Management (ITSM*).

A1.42. Authority for ensuring DAF information technology, platform information technology (also known as operational technology), and NSS comply with DoD cybersecurity policies and procedures, as delegated to SecAF pursuant to DoDI 8500.01, *Cybersecurity*.

A1.43. Authority for managing security and cybersecurity technical risks and vulnerabilities, providing procedures for protection of risk, and complying with Risk Management Framework for DoD information technology and platform information technology (also known as operational technology) under the DAF's purview, as delegated to SecAF pursuant to DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT).*

A1.44. Authority for planning, programming, and budgeting to support the evolution of the DoD Public Key Infrastructure program and to public key-enable applicable DAF information systems as required, as delegated to SecAF pursuant to DoDI 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*.

A1.45. Authority for planning, programming, and budgeting to support and ensure proper use of identity authentication processes for DAF information systems and networks, as delegated to SecAF pursuant to DoDI 8520.03, *Identity Authentication for Information Systems*.

A1.46. Authority for appropriately complying with DoD-approved policies, standards, processes, and procedures for collection, transmission, storage, archiving, caching, tagging, retrieval, and interoperation of biometric capabilities, as delegated to SecAF pursuant to DoDD 8521.01E, *DoD Biometrics*.

A1.47. Authority for implementing all applicable communications security policies, directives, criteria, and standards within the DAF, as delegated to SecAF pursuant to DoDI 8523.01, *Communications Security*.

A1.48. Authority for developing DAF-specific cybersecurity requirements to support provision of protection capabilities within the DAF portions of the DODIN, as delegated to SecAF pursuant to DoDI 8530.01, *Cybersecurity Activities Support to DoD Information Network Operations.*

A1.49. Authority for establishing a Cross Domain Support Element (CDSE) to carry out CDSE responsibilities for DAF current or planned cross domain solutions (CDS); appoint representatives to the Cross Domain Technical Advisory Board (CDTAB); oversee and monitor the life cycle management of DAF CDSs and CDS security configurations in compliance with DoD policy, as delegated to SecAF pursuant to DoDI 8540.01, *Cross Domain (CD) Policy*.

A1.50. Authority for providing guidance and overseeing information technology implementation to ensure ports, protocols, and services are properly used, assessed, declared, implemented, regulated, verified, documented, and approved in compliance with DoD policy, as delegated to SecAF pursuant to DoDI 8551.01, *Ports, Protocols, and Services Management (PPSM).*

A1.51. Authority for ensuring cybersecurity is implemented in all system and service acquisitions in accordance with issued DoD guidance, and in coordination with service acquisition executives, as delegated to SecAF pursuant to DoDI 8580.1, *Information Assurance (IA) in the Defense Acquisition System*.

A1.52. Authority for ensuring unclassified DoD information provided to or developed by non-DoD entities is protected by including requirements implementing DoD policy in contracts, grants, and other legal agreements, as delegated to SecAF pursuant to DoDI 8582.01, *Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information*.

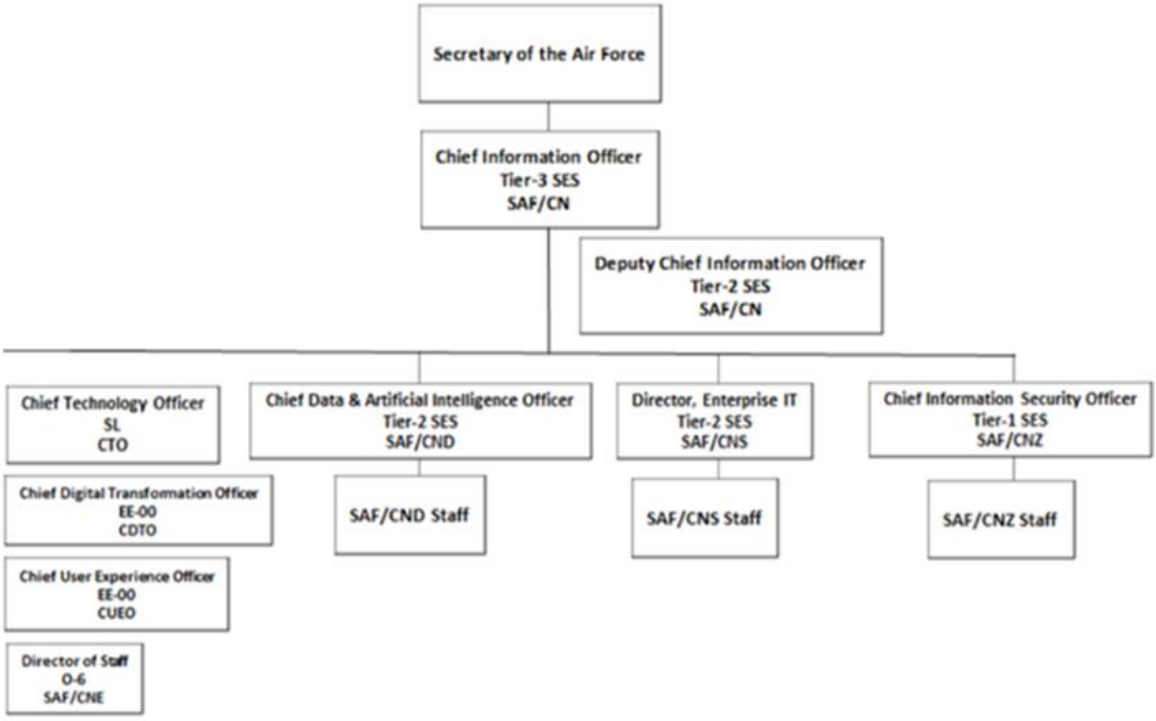
A1.53. Authority for establishing the DAF information collections control and reporting activity consistent with Office of Management and Budget requirements, as delegated to SecAF pursuant to DoDI 8910.01, *DoD Implementation of the Paperwork Reduction Act,* and DoD Manual 8910.01, Volumes 1 & 2, *Information Collection and Reporting*.

A1.54. Responsibility for ensuring that DAF AI and RAI activities are conducted consistent with Department of Defense policies, as assigned to the SecAF in Deputy Secretary of Defense Memorandum, *Implementing Responsible Artificial Intelligence in the Department of Defense*, dated May 26, 2021.

ATTACHMENT 2

CHIEF INFORMATION OFFICER

(SAF/CN)



A2.1. The Chief Information Officer (SAF/CN) has responsibility for information technology, cybersecurity, enterprise data management, AI policy and governance, information management, and information resources management for the DAF. The portfolio includes oversight and management of unclassified, classified (non SCI/intel), and SAP information technology in support of both the U.S. Air Force and U.S. Space Force. The SAF/CN mission is to deliver the rock-solid digital foundation on which the future U.S. competitive advantage relies, and to equip Airmen and Guardians with the knowledge, tools, and data they need to fight.

A2.2. The Deputy Chief Information Officer (SAF/CN DCIO) assists the DAF Chief Information Officer with all assigned responsibilities for the DAF. The DCIO is also responsible for oversight of the Chief Technology Officer (SAF/CN CTO), Chief Digital Transformation Officer (SAF/CN CDTO), Chief Experience Officer (SAF/CN CXO), Guard & Reserve Assistants (SAF/CN GRA), and Executive Services (SAF/CNE).

A2.3. Three-letter subordinate offices and advisors include:

A2.3.1. The Chief Data and Artificial Intelligence Officer (SAF/CND), colloquially referred to as DAF CDAO to better align with OSD, in addition to the responsibilities in **paragraph 3.23** The CDAO is the Chief Data Officer and has responsibilities as set forth in 44 USC 3520. The CDAO is responsible for leading, carrying out, reviewing, and ensuring data in the DAF is visible, accessible, understandable, linked, trustworthy, interoperable, and secured (VAULTIS). The CDAO establishes strategic direction and guidance for management of DAF data throughout its lifecycle. The CDAO also prepares policies and issues guidance to ensure implementation of data governance across the enterprise. The CDAO assesses the readiness, efficiency, and scale at which the DAF is able to leverage data as a strategic asset to inform digital modernization strategies, as well as shape a collaborative data-driven environment. The CDAO significantly contributes to AI initiatives to address the DAF's critical focus on AI policy development and governance implementation. The CDAO annually collates this information into an evaluation of compliance for report to Congress, pursuant to 44 USC § 3520(e). Additionally, the CDAO represents DAF interests in Office of the Secretary of Defense and Federal CDAO forums, policy creation, and strategy discussions.

A2.3.2. The Director of Enterprise Information Technology (SAF/CNS) is responsible for matters pertaining to providing policy, guidance, and oversight for processes and procedures associated with information technology governance and partner engagement. SAF/CNS manages the DAF enterprise information technology portfolios. SAF/CNS leads development of EIT budgets and consolidates reporting for all DAF information technology and cyber activities budgets. SAF/CNS serves as the principal information technology and platform information technology (also known as operational technology) subject matter expert and advocates for related requirements in mission system modernization. SAF/CNS manages and coordinates SAF/CN equities in the U.S. Air Force and U.S. Space Force requirements processes and in DAF and DoD requirements governing bodies. SAF/CNS also manages and coordinates SAF/CN equities in DAF and DoD architecture governing bodies.

A2.3.3. The Chief Information Security Officer (SAF/CNZ) is responsible for oversight and policy guidance for cybersecurity and cybersecurity risk management of unclassified, classified (non SCI/intel), and Special Access Programs (SAP) information technology in support of both the U.S. Air Force and U.S. Space Force missions. SAF/CNZ partners with DAF, CIO, Joint, and Federal agencies to support an integrated approach to cybersecurity that effectively manages community risk while meeting Department and Service needs. SAF/CNZ develops, maintains, monitors/reports and enforces compliance with cybersecurity policies, guidance, standards, Congressional mandates, and statutory requirements. SAF/CNZ also develops and manages CISO governance and compliance frameworks as well as leads DAF equities in DoD interoperability governing bodies.

A2.3.4. The Chief Technology Officer (SAF/CN CTO) is responsible for advising the DAF CIO on cybersecurity and IT emerging technology, enterprise architecture, enterprise infrastructure, and strategy including identifying short- and long-term goals of Department-wide cybersecurity and IT initiatives. The CTO provides executive and senior level technical leadership, direction and oversight of Department-wide large-scale IT issues and initiatives, ensuring the integrity, interoperability, supportability, and cost-effectiveness of the Department's IT and provides advice to HAF, Major Commands (MAJCOM), and Field Commands (FLDCOM) on cybersecurity and IT issues, activities and impacts.

A2.3.5. The Chief Digital Transformation Officer (SAF/CN CDTO) is responsible for measurably increasing the use of digital technologies across the Department. The CDTO works with partners across the DAF and connects, champions, and enables digital initiatives that can significantly impact the organization.

A2.3.6. The Chief Experience Officer (SAF/CN CXO) is responsible for improving DAF members' user experience, transforming Department systems through human-centered design, and integrating user experience feedback, continuously optimizing technology to improve warfighter effectiveness. The CXO also measures and improves performance and experience data, and develops and leverages the right metrics to provide the best aggregate value user experience for warfighter effects.

A2.3.7. Air National Guard and Air Force Reserve Assistants (SAF/CN GRA) are responsible for advising the CIO on matters impacting Air Reserve Component (ARC) information technology, funding, and associated cyberspace operations units and personnel. The ARC advisors also support CIO strategic initiatives that pertain to Total Force integration, synchronization, and mobilization.

A2.3.8. Executive Services (SAF/CNE) is comprised of the Director of Staff (DoS) and the Director's Action Group (DAG). The Executive Services offices are responsible for supporting the SAF/CN principals with strategy development, strategic communications, and preparation for external engagements. Executive Services also support the SAF/CN staff through administrative processes and support, task management, prioritization, and tracking.