

**BY ORDER OF THE
SECRETARY OF THE AIR FORCE**

HAF MISSION DIRECTIVE 1-26



5 FEBRUARY 2015

**CHIEF, INFORMATION DOMINANCE AND
CHIEF INFORMATION OFFICER**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at www.e-Publishing.af.mil for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/CIO A6SS

Certified by: SAF/CIO A6
(Lt Gen William J. Bender)

Supersedes: HAF MD1-26, 22 June 2011

Pages: 28

SUMMARY OF CHANGES. This revision includes significant changes due to the Headquarters Air Force (HAF) reorganization. In addition, it adds references to newly promulgated Department of Defense issuances, and removes or changes references that have been superseded, changed, or rescinded; updates organizational responsibilities; enhances certain descriptions to more accurately reflect pertinent references; and incorporates minor administrative changes for grammar and readability.

1. Mission. The Secretary of the Air Force (SecAF), pursuant to 10 United States Code (USC) §§ 8013-8016, may establish offices and officials within the Secretariat to assist the Secretary in carrying out his or her responsibilities. As documented by Paragraph 4.1 of AFMD-1, *Headquarters Air Force*, and this Headquarters Air Force Mission Directive, the Chief, Information Dominance and Chief Information Officer (SAF/CIO A6) is established as part of the Secretariat. The SAF/CIO A6 has overall responsibility for cyberspace/Information Technology (IT) policies and concepts; enterprise-wide integration of Air Force cyberspace/IT, including National Security Systems (NSS); information resources management (IRM); spectrum management; information management (IM); knowledge management (KM); postal operations; cybersecurity; warfighting integration; and related matters for the Department of the Air Force, pursuant to 10 USC § 2223, 40 USC § 11315, and 44 USC §§ 3506 and 3544. The SAF/CIO A6 serves as the Department of the Air Force Enterprise-level strategist and business advisor from the cyberspace/IT and IRM perspective; Information architect for the Department

of the Air Force enterprise; and Air Force-wide IT/IRM executive. The SAF/CIO A6 is the Functional Authority for 17X, 1BX, 3DX, 3A career fields and occupational series assigned by the SecAF. The SecAF retains ultimate responsibility for all policies related to the Department of the Air Force. Within his/her areas of responsibility, SAF/CIO A6 prepares policies for approval and issues official guidance via official Department of the Air Force 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 Department of the Air Force. The Secretariat, the Chief of Staff of the Air Force (CSAF), and Air Staff offices perform their Department of the Air Force functions subject to the authority, direction and control of the SecAF.

2.1. The SAF/CIO A6 reports directly to the SecAF as the Department's Chief Information Officer, advises CSAF, serves as an agent of the SecAF within assigned policy and program domains, and provides direction, guidance and oversight for all matters pertaining to the formulation, review, and execution of plans, policies, programs, doctrine, and budgets within his/her areas of responsibility. The SAF/CIO A6 is accountable to the SecAF for results achieved within the policy and program domains assigned by this Directive.

2.2. The SAF/CIO A6 is a member of the Secretariat and as such works closely with other HAF offices to assist the SecAF in carrying out his/her responsibilities. The SAF/CIO A6 and the Office of the SAF/CIO A6 work in cooperation with the CSAF, Vice Chief of Staff, the Under Secretary of the Air Force (SAF/US), the Assistant Secretaries of the Air Force and their respective offices as well as other HAF organizations which are responsible, pursuant to Chapters 803 and 805 of Title 10 (10 USC §§ 8013-8023 and §§ 8031-8038) 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 Directive – Delegations of Authority and Assignment of Responsibilities*, two or more HAF two-letter/digit organizations with responsibilities in the same functional area are encouraged to develop standard operating procedures (SOPs) that set forth procedures enabling covered organizations to fulfill and carry out their respective missions, roles, and responsibilities. Currently, there is one SOP between SAF/CIO A6 and AF/SE included at **Attachments 3**. SAF/CIO A6 will initiate SOPs as necessary for functional responsibilities shared with other organizations.

3. Responsibilities. The SAF/CIO A6 is specifically responsible for:

3.1. Serving as the sole Department of the Air Force Chief Information Officer pursuant to 10 USC § 2223, 40 USC § 11315, and 44 USC §§ 3506 and 3544. Advising and assisting the SecAF, CSAF, and other HAF offices on policy and issues regarding all assigned responsibilities and functions as they relate to the Air Force. SAF/CIO A6 may designate subordinate CIOs, but a reporting mechanism must be maintained through the SAF/CIO A6 to ensure continuity of purpose in accordance with (IAW) DoD Directive (DoDD) 8000.01, *Management of the Department of Defense Information Enterprise*.

3.2. Enabling an operationally-resilient, reliable and secure cyberspace domain to meet Air Force mission needs. The cyberspace domain provides the foundation for the development and delivery of integrated support in each of the four defined Department of Defense (DoD) mission areas (MA): Warfighting (WMA), Business (BMA), Information Environment

(IEMA), and Defense Intelligence (DIMA). SAF/CIO A6 will lead Air Force-wide councils and boards involving CIO matters across these four mission areas.

3.3. Delivering the vision for the Air Force Information Environment (IE) informed by DoD, Joint, and Air Force priorities to include directing standards for the construction and use of IE capabilities for meeting Air Force warfighting and business requirements and aligning Air Force policies and efforts with DoD initiatives such as the Joint Information Environment (JIE) to meet and integrate Air Force and Joint/Coalition warfighting requirements. The strategic direction will guide investments to meet Air Force core mission needs.

3.4. Developing and maintaining an Air Force Information Dominance Flight Plan aligned with the Air Force Strategic Master Plan (SMP) and associated annexes to inform mission area roadmaps and core function support plans.

3.5. Establishing and maintaining an Air Force CIO policy office to oversee the implementation of public laws, publications and policies, and compliance as they pertain to duties delineated in this Mission Directive and consistent with DoD enterprise-level defense strategies from the cyberspace/IT, IM, and NSS perspectives.

3.6. Providing corporate investment inputs to achieve desired core mission capabilities through operations of the Information Technology Governance Executive Board (ITGEB). The SAF/CIO A6 will establish a fully integrated, flexible, modularized, open and net-centric family of systems, networks and architectures bridging theater warfighting, combat support, global/functional capabilities and infrastructure enterprises through operations of the Warfighting Integration (WFI) General Officer Steering Group (GOSG).

3.6.1. Coordinate with other HAF offices to assist the SecAF and the CSAF in carrying out their responsibilities. SAF/CIO A6 will coordinate closely with HAF offices of primary responsibility (OPR) for designated functional expertise to include planning, programming, policy, guidance, and force development for both the active and reserve components; and in developing strategy, guidance standards, and concepts of operations for capabilities and programming flight plans/roadmaps.

3.6.2. Review the performance of the Air Force IT and NSS programs (to include monitoring and evaluating the performance of IT and NSS programs on the basis of all applicable performance measurements). Provide recommendations on the continuation, modification, or termination of cyberspace, IT, and/or NSS programs or projects pursuant to 40 USC § 11315, 44 USC § 3506, 44 USC § 3541, et seq. (the Federal Information Security Management Act of 2002), 44 USC § 3603, and other applicable authorities.

3.6.3. Advocate for Air Force interests as a co-principal representative with the SAF/US(M) in the Defense Business Council.

3.7. Serving as Department of the Air Force cyberspace/IM/IT Portfolio Manager in coordination with the operational and resource management stakeholders.

3.7.1 Establish and maintain a coherent cyberspace/IM/IT Capital Planning and Investment Management process for integrated, efficient, and effective allocation of resources.

3.7.2 Ensure that the cyberspace/IM/IT Capital Planning and Investment Management process is integrated with planning, programming, budgeting, financial, strategic sourcing, and program management processes.

3.7.3. Review Air Force budget requests for cyberspace/IT and NSS pursuant to 10 USC § 2223 and develop a full and accurate accounting (in concert with SAF/FM) of IT expenditures, related expenditures & results pursuant to 44 USC § 3506 and 40 USC § 11315.

3.7.4 Ensure cyberspace/IT investments are aligned with Air Force strategy and capability delivery in coordination with the operational and resource management stakeholders.

3.7.5. Provide for the elimination of duplicate cyberspace/IT and NSS within and between the DoD Components, including the Military Departments and the Defense Agencies.

3.8. Serving as the Department of the Air Force Chief Architect for the Air Force portion of the DoD Information Network (DoDIN) and providing oversight, analysis, and policy guidance to ensure compliance with standards for developing, maintaining, and implementing sound integrated and interoperable architectures across the Air Force. Ensure that information security protections are integrated into architectures pursuant to 44 USC § 3534 and 40 USC § 11315.

3.8.1. Maintain an Air Force Enterprise Architecture (EA), including a technical reference model and standards profile, as part of the DoD EA.

3.8.2. Ensure the cyberspace/IT investments are aligned with the Air Force EA planning processes, using a disciplined capital planning and investment control (CPIC) process to acquire, use, maintain, and dispose of IT.

3.9. Coordinating with Joint Staff and the Office of the Secretary of Defense (OSD) on cyberspace/IM/IT/NSS matters to ensure consistency with JIE and DoDIN strategies, policies, and guidance.

3.9.1. Represent the Air Force in Joint fora (e.g., Joint Satellite Communications (SATCOM) Panel) related to cyberspace, information, and WFI as directed by the CSAF, Chairman of the Joint Chief of Staff (CJCS), or DoD issuances.

3.9.2. Develop the Air Force position on issues related to cyberspace/IM/IT/NSS capabilities in support of the Joint Capabilities Integration and Development System.

3.9.3. Conduct internal Air Force coordination and represent the Air Force to the Joint community on matters related to Joint Command and Control.

3.9.4. Serve as the Air Force representative for Net-Centric (NC) Joint Capability Area portfolio management. Represent the Air Force NC capability portfolio during Air Force Corporate Structure (AFCS) processes. Advise the AFCS panels, Group, Board, and Council on NC capability priorities, strategy and investments.

3.9.5. Provide guidance and direction in coordination with AF/A2, AF/A3, AF/A5/8 AF/A10, and SAF/AQ, through AF Program Executive Officer (AFPEO) Command, Control, Communication, Intelligence and Networks (C3I&N), to synchronize and

integrate Cyberspace, Intelligence, Surveillance and Reconnaissance (ISR), Command and Control (C2), and Nuclear Command, Control & Communications (NC3) capabilities and requirements and to promote and improve interoperability, supportability, and information sharing.

3.9.6. Provide oversight of Air Force Spectrum Management policy and guidance in coordination with Core Function Leads and the Air Force Spectrum Management Office.

3.9.7. Facilitate the availability of authoritative data to the Air Force network enterprise and make Air Force authoritative data available to other mission partners.

3.9.8. Identify and prioritize Air Force WFI issues in coordination with Core Function Leads, other Air Staff offices and Joint commands. Develop support planning, programming, and policy guidance to optimize the Department of the Air Force's combat effectiveness, subject to fiscal constraints.

3.9.9. Provide oversight on the establishment of policies, procedures, and execution of the Air Force Cryptographic implementation and modernization efforts.

3.10. Performing duties and fulfilling the responsibilities associated with information security, cybersecurity, and other matters prescribed by 44 USC Chapter 35, Subchapter III.

3.10.1. Appoint a Senior Information Security Official (SISO) in accordance with 44 USC § 3544.

3.10.2. Appoint Air Force Authorizing Officials on behalf of SecAF.

3.11. Serving as a principal member of the Special Access Program Oversight Committee.

3.12. Serving as the Cyberspace Operations and IM Functional Authority for both the military and civilian career fields pursuant to 40 USC § 11315, 44 USC §§ 3506 (b)(5) and 44 USC §§ 3544 (a)(3)(D).

3.12.1. Provide the policy and guidance necessary to develop the total Cyberspace Operations and IM workforce.

3.12.2. Determine and establish knowledge and skill requirements necessary for personnel to accomplish their missions.

3.12.3. Evaluate force structure and the effect on in-garrison and deployed operations.

3.13. Serving as the focal point for Air Force-wide issues regarding IM, knowledge operations management, information access, information formats to include data structures and postal operations.

3.13.1. Approve guidance for the development and staffing of IM policy and guidance across the Department of the Air Force.

3.13.2. Serve as the designated Chief Freedom of Information Act (FOIA) Officer, with responsibility for efficient and appropriate compliance with 5 USC § 552.

3.13.3. Establish and provide policy oversight and guidance for a FOIA office created to ensure Air Force compliance with 5 USC §§ 552.

3.13.4. Establish and provide oversight for a Privacy and Civil Liberties office created to ensure Air Force compliance with 5 USC §§ 552a, Public Law 107-347, "The E-

Government Act of 2002”, and Public Law 110-53, “*Implementing Recommendation of 9/11 Commission Act of 2007*”. Serve as the Air Force Senior Agency Official for Privacy with responsibility for information privacy issues as described by Office of Management and Budget (OMB) Memoranda 05-08, “*Designation of Senior Agency Officials for Privacy*”.

3.13.5. Establish and provide oversight for a Records Management office pursuant to 44 USC Chapter 31, (“Federal Records Act”, as amended) and appoint a Senior Records Management Official according to OMB Memoranda 12-18, *Managing Government Records Directive*.

3.13.6. Ensure compliance with the FOIA, the Computer Matching and Privacy Act, Records Management and Federal Register requirements.

3.13.7. Establish and provide oversight for an Information Collections and Reports office created to ensure Air Force compliance with Federal Information Policy, as set forth in 44 USC Chapter 35, Subchapter I.

3.13.8. Establish and provide oversight for a Section 508 office created to ensure Air Force compliance with the requirements of 29 USC §§ 794d.

3.14. Developing cyberspace policies and submitting them for coordination and concurrence prior to SecAF approval. SAF/CIO A6 shares with the Deputy Chief of Staff, Operations (AF/A3) responsibility for providing policy, guidance, and oversight for Cyberspace Operations through a matrixed staff activity. Coordinate the efforts of the operations and cyberspace communities at the Service level to ensure that operational requirements are considered in all decisions affecting cyberspace activities.

3.14.1. Certify through the matrixed staff activity purposed cyberspace operations policies on behalf of AF/A3 prior to SAF/CIO A6 approval.

3.14.2. Integrate the activities of the Air Force’s operations, ISR, and cyberspace communities to ensure the delivery of Air Force cyberspace operational capabilities to Air Force warfighters and joint warfighting components.

3.14.3. Ensure operational assessment of current and future cyberspace operations and information superiority capabilities are integrated in the Air Force Capability Based Planning Process. Provide cyberspace/IT and WFI subject matter expertise to support Air Force strategic and contingency planning.

3.14.4. Advise and assist in the development, coordination, and integration of strategy, doctrine and guidance for cyberspace operations capabilities into Air Force, Joint, Combatant Command, Coalition, and national planning and operations.

3.15. Advocating and providing oversight for the development of integrated aerial layer networks that are modular, based on open standards, and interoperable with the joint community.

3.16. Advocating and ensuring SAF/CIO A6 equities are endorsed at the Air Force Requirements Oversight Council (AFROC) and Joint Requirements Oversight Council (JROC).

3.16.1. Ensures effective and efficient IT management as required by Congressional, statutory and DoD regulatory requirements (e.g., Clinger Cohen Act and DoD 5000 series, CJCS Instruction (CJCSI) 6212.01).

4. Delegations of Authority/Assignment of Responsibility: Attachment 1 lists delegated authorities and assigned responsibilities to SAF/CIO A6. The authorities delegated and responsibilities assigned to the SAF/CIO A6 by this HAF Mission Directive may generally be re-delegated unless re-delegation is expressly prohibited by the attached delegation or superseding law, regulation, or DoD issuance. While the SAF/CIO A6 may re-delegate authorities to other Department of the Air Force officials, he or she will ultimately be responsible to the SecAF for all matters listed in **paragraph 1** of this publication. Any re-delegation of authority/assigned responsibility made shall not be effective unless it is in writing. Any person re-delegating authority in accordance with this HAF Mission Directive may further restrict or condition the authority/assigned responsibility being re-delegated.

5. Notifications to Congress: No re-delegation of authority/assigned responsibility under this HAF Mission Directive below the level of Deputy Assistant Secretary or three-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 HAF Mission Directive remain effective insofar as such re-delegations are not inconsistent with the terms of this HAF Mission Directive unless superseded by a new re-delegation or assignment of responsibility.

DEBORAH LEE JAMES
Secretary of the Air Force

Attachments:

1. Delegations of Authority/Assignments of Responsibility for SAF/ CIO A6
2. SAF/CIO A6 Organizational Chart
3. Standard Operating Procedure for SAF/CIO A6 and AF/SE

ATTACHMENT 1**DELEGATIONS OF SECRETARY OF THE AIR FORCE
AUTHORITY/ASSIGNMENTS OF RESPONSIBILITY
TO THE
CHIEF, INFORMATION DOMINANCE AND
CHIEF INFORMATION OFFICER (SAF/CIO A6)**

A1.1. Authority to issue general regulations making punishable pursuant to 10 USC Chapter 47 (UCMJ), reprisals or the threat of reprisals by persons subject to the UCMJ against individuals who make complaints or disclose information that indicates a possible violation of privacy protections or civil liberties in the administration of the programs and operations of the Federal Government to designated personnel, designate a senior Service member or civilian employee to serve as the Air Force chief civil liberties officer, designate a Service member or civilian employee to serve as the Air Force primary civil liberties point of contact, periodically investigate and review Air Force actions, policies, procedures, guidelines, and related laws and their implementation to ensure that the Air Force is considering appropriate privacy and civil liberties, ensure the Air Force has adequate procedures to receive, investigate, respond to, and redress complaints from individuals who allege that the Air Force violated their privacy or civil liberties; ensure advice on proposals to retain or enhance a particular governmental power considers whether the AF has established that the need for the power is balanced with the need to protect privacy and civil liberties, there is adequate supervision of the use by the Air Force of the power to ensure protection of privacy and civil liberties, and there are adequate guidelines and oversight to properly confine the use of the power; coordinate privacy and civil liberties activities with the Air Force Inspector General to avoid duplication of effort; ensure reprisals by civilian employees that involve allegations of civil liberties or privacy protection violations are appropriately reviewed for disciplinary action; submit reports; and ensure Air Force employees and Service members are trained regarding the protection of privacy and civil liberties as delegated to the Secretary of the Air Force, pursuant to Department of Defense Instruction (DoDI) 1000.29, *DoD Civil Liberties Program*.

A1.2. Authority relating to the conduct of periodic reviews of Social Security Number (SSN) use and reporting on the results of such review and justifications for all forms and systems as delegated to the Secretary of the Air Force, pursuant to DoDI 1000.30, *Reduction of Social Security Number (SSN) Use within DoD*.

A1.3. Authority relating to implementing Electromagnetic Environmental Effects (E3) control requirements during acquisition processes, to include the implementation and tailoring of Military Standard (MIL-STD)-461F and electromagnetic radiation (EMR) hazards criteria; performing E3 control assessments; addressing and mitigating identified E3 issues; addressing Hazards of Electromagnetic Radiation to Ordnance (HERO) requirements and providing data to the Director, Defense Spectrum Organization (DSO); coordinating within the DoD E3 Integrated Product Team (IPT) on the development of analytical tools or services to predict, assess, and

mitigate E3 problems; implementing E3 control procedures to maintain electromagnetic compatibility (EMC) at designated DoD sites, advising the Director, DSO, of requests for installation, and providing results of EMC analyses; implementing E3 education and awareness training and coordinating training requirements with DoD E3 IPT; documenting CREW system, subsystem, and equipment limitations and vulnerabilities for unresolved E3 control problems and reporting the results during operational interoperability and compatibility decisions; and assigning a representative to the DoD E3 as delegated to the Secretary of the Air Force, pursuant to DoDI 3222.03, *DoD Electromagnetic Environmental Effects (E3) Program*.

A1.4. Authority relating to directing program managers and functional item managers to use a common CM approach to establish and control product attributes and technical baselines across the total system life cycle; and directing program managers to identify, document, audit, and control the functional and physical characteristics of the system designs, track changes, and provide an audit trail of program design decisions and design modifications; coordinating with the National Leadership Command Capabilities (NLCC) Configuration Manager for Configuration Management (CM) reporting requirements; requiring program managers and functional item managers to identify configuration item databases pertinent to NLCC systems and make those databases accessible to the NLCC Configuration Manager for either automated data capture or direct report; ensuring all new or extant industry contracts include required CM data provisions; reviewing proposed CM changes; reviewing NLCC system configuration database and reporting discrepancies; and participating in the NLCC Configuration Control Board (CCB) process as delegated to the Secretary of the Air Force, pursuant to DoDI 3741.01, *National Leadership Command Capabilities (NLCC) Configuration Management (CM)*.

A1.5. Authority relating to delineating the Air Force's roles and responsibilities, resourcing, technical solutions, and operations for implementation of Senior Leader Secure Communications Modernization (SLSCM) policies and strategies; ensuring applicable Air Force policies, guidance, and strategies align with the posture and direction of SLSCM strategies and plans; planning, programing, & budgeting for SLSCM capabilities; developing coordinated position of resource impact(s) for modernization recommendations with the other Services through the Joint Staff Action Process; developing plans to replace current voice, video, and data capabilities with IP-based broadband capabilities that meet senior leadership operational requirements and approving, procuring, and deploying approved material solutions IAW federal and Air Force acquisition rules as delegated to the Secretary of the Air Force, pursuant to DoDI O-3780.01, *Senior Leader Secure Communications Modernization (SLSCM)*, marked as For Official Use Only (FOUO).

A1.6. Authority relating to requesting the establishment and operation of Military Post Offices (MPO); maintaining inspection, advisor, and assistance responsibilities; coordinating air and surface transportation support; and providing and maintaining military personnel and information systems support to the Military Postal Service (MPS) Agency (MPSA) as delegated to the Secretary of the Air Force, pursuant to DoDI 4525.7, *Military Postal Service and Related Services*.

A1.7. Authority relating to the appointment of Official Mail Managers (OMM) and implementation of the DoD Official Mail Program (OMP) as delegated to the Secretary of the Air Force, pursuant to DoDI 4525.08, *DoD Official Mail Management*.

A1.8. Authority relating to implementation during the systems acquisition process or for communications waveform modifications by providing subject matter expert support as delegated to the Secretary of the Air Force, pursuant to DoDI 4630.09, *Wireless Communications Waveform Development and Management*.

A1.9. Authority relating to designating officials to monitor, document, and maintain records of telecommunications expenditures and submitting required DD Forms 448; designating one or more Telecommunications Service Control Officers (TSCO); ensuring internal management controls are implemented to safeguard telecommunications assets, including the certification of bills; providing the Director, United States Army Information Technology Agency (USAITA), required copies of all long-haul telecommunications service requests; and assuming responsibility for payment of costs associated with telecommunications support as delegated to the Secretary of the Air Force, pursuant to DoDI 4640.07, *Telecommunications Services in the National Capital Region (NCR)*.

A1.10. Authority relating to providing spectrum management; developing procedures to implement and implementing spectrum management policies; promoting the use of innovative spectrum-efficient technologies and development of systems that can operate in diverse electromagnetic environments (EMEs); using DoD joint standard spectrum management information systems, databases, analytical tools and information exchange formats; developing, maintaining, and enhancing spectrum-related analytical tools to support unique Air Force capabilities; providing representatives to the Interdepartmental Radio Advisory Committee; providing requested or otherwise authorized representation at other spectrum-related forums; ensuring the Air Force's spectrum management interests are represented on the Military Command, Control, Communications, and Computers Executive Board (MC4EB) (successor to Military Communications Electronics Board) and its panels and working groups; and developing and maintaining a cadre of qualified spectrum management personnel as delegated to the Secretary of the Air Force, pursuant to DoDI 4650.01, *Policy and Procedures for Management and Use of the Electromagnetic Spectrum*.

A1.11. Authority relating to encouraging participation in the Military Auxiliary Radio System (MARS); ensuring that MARS capabilities established are available and mutually interoperable; encouraging MARS participation in the Shared Resources High Frequency (HF) Radio Program; planning and executing specific communications missions for any established MARS capabilities; establishing programs to promote civilian interest; and providing an annual report to the DoD CIO as delegated to the Secretary of the Air Force, pursuant to DoDI 4650.02, *Military Auxiliary Radio System (MARS)*.

A1.12. Authority relating to encryption of imagery transmitted by airborne systems and unmanned aircraft control communications as delegated to the Secretary of the Air Force, pursuant to DoDI 4660.04, *Encryption of Imagery Transmitted by Airborne Systems and Unmanned Aircraft Control Communications (U) (Classified)*.

A1.13. Authority relating to establishing and maintaining the DoD Records Management Program at an organizational level sufficient to efficiently and effectively implement DoD objectives and policies; designating a Records Management Program administrator; applying standards, procedures, and techniques designed to improve the management of records; ensuring records are created, maintained and preserved in accordance with DoD policy; using the most economical, efficient, and reliable means for creation, retrieval, maintenance, preservation, and

disposition of records in any media; improving the management, maintenance, and security of records in coordination with OSD and the CJCS; applying DoD records management functional and system requirements to all electronic records management systems; incorporating records management requirements into automated information systems development and redesign; ensuring proper training of all personnel that create and use records; advising employees of their responsibilities; ensuring proper disposition of records; evaluating Air Force compliance with the DoD Records Management Program and Federal regulations; advising Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) of records management issues with extra-Air Force implications and cooperating with ASD(C3I) in resolving such issue; and safeguarding all personal data within records as delegated to the Secretary of the Air Force, pursuant to Department of Defense Directive (DoDD) 5015.2, *DoD Records Management Program*.

A1.14. Authority relating to referring military communications-electronics and NSS matters to the Military Command, Control, Communications, and Computers Executive Board (MC4EB) (successor to Military Communications Electronics Board) for coordination, or other applicable action; and providing qualified personnel when requested by the Chair, MC4EB, to serve on subsidiary MC4EB panels as delegated to the SecAF, pursuant to DoDD 5100.35, *Military Communications-Electronics Board (MCEB)*.

A1.15. Authority relating to Defense and national leadership command capability as delegated to the Secretary of the Air Force pursuant to DoDI S-5100.92, *Defense and National Leadership Command Capability (DNLCC) Governance* (U), marked as Secret.

A1.16. Authority relating to ensuring the OMP is considered in the budgeting process to maintain a sufficient number of trained and experienced personnel to meet OMP requirements and to cover mail costs; coordinating with the MPSA on contingency and exercise planning for mail support; submitting all policy exception and agreement requests through the MPSA for DoD approval; including postal subject matter experts in the requirements determination and technical review process for contracts containing postal matters and postal facility plans impacting the MPS and OMP; providing representatives to the MPS and OMP Corporate Boards, as applicable and ensuring attendance at meetings; submitting annual mail management report information to the DoD Official Mail Manager; providing required postal service; programming, budgeting, and obligating funds for Air Force mail costs; providing required MPSA staff; ensuring Air Force military postal policy and management functions do not duplicate MPSA responsibilities; providing an adequate number of trained personnel for worldwide MPS and OMP operations; and providing required transportation support and reimbursement as delegated to the Secretary of the Air Force, pursuant to DoDD 5101.11E, *DoD Executive Agent for the Military Postal Service (MPS) and Official Mail Program (OMP)*.

A1.17. Authority relating to advising and coordinating with Director, Defense Information Systems Agency (DISA) regarding funding shortfalls, program activities, programmatic documents and technical specifications, standards, and acquisition plans; and identifying requirements for DISA support for networks, telecommunications, and IT systems, services, and capabilities as delegated to the Secretary of the Air Force, pursuant to DoDD 5105.19, *Defense Information Systems Agency (DISA)*.

A1.18. Responsibility for coordinating with the DoD CIO on all matters under the Air Force's purview relating to identified authorities, responsibilities and functions as assigned to the

Secretary of the Air Force pursuant to DoDD 5144.02, *DoD Chief Information Officer (DoD CIO)*.

A1.19. Authority relating to communications security measures used in nuclear command and control communications as delegated to the Secretary of the Air Force, pursuant to DoDI S-5200.16, *Objectives and Minimum Standards for Communications Security (COMSEC) Measures Used in Nuclear Command and Control (NC2) Communications*, marked as Secret.

A1.20. Authority relating to controlling access to classified cryptographic information, carrying out and administering a cryptographic access program; carrying out a counterintelligence scope polygraph examination program; maintaining records on individuals granted cryptographic access and those who have had such access withdrawn; accepting cryptographic access granted by other DoD Components; denying or withdrawing cryptographic access to those individuals who fail to agree to or comply with specified criteria; and incorporating cryptographic access policy into appropriate training and awareness programs as delegated to the Secretary of the Air Force, pursuant to DoDI 5205.08, *Access to Classified Cryptographic Information*.

A1.21. Authority relating to supporting planning, programming, resourcing, and budgeting for Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) activities; ensuring acquisition programs support DIB CS/IA activities in accordance with public law and acquisition regulations; developing procedures and conducting cyber intrusion damage assessments in support of DIB CS/IA activities and consistent with Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) policy guidance; and serving as the DoD Executive Agent (EA) for DC3 digital forensic training and laboratory services as delegated to the Secretary of the Air Force, pursuant to DoDI 5205.13, *Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities*.

A1.22. Authority relating to obtaining document services through Defense Logistics Agency (DLA) Document Services and providing necessary information and assistance to the Director, DLA (successor to Director, DAPS) as delegated to the Secretary of the Air Force, pursuant to DoDI 5330.03, *Defense Logistics Agency (DLA) Document Services*.

A1.23. Authority relating to internally administering the FOIA Program and publishing necessary instructions; serving as, or appointing another Air Force official as, the FOIA appellate authority; establishing a FOIA Request Service Center; establishing prescribed FOIA Requester Service Centers; submitting names of personnel to the Director, Administration and Management (DA&M) for designation as FOIA Public Liaisons; ensuring identified agency officials are made aware of FOIA requests and releases that may be of significant public, media, or Congressional interest or of interest to senior DoD officials; conducting required training; ensuring FOIA Public Liaisons submit required reports; making records available as required; and maintaining and making current indices of such records as delegated to the Secretary of the Air Force pursuant to DoDD 5400.07, *DoD Freedom of Information Act (FOIA) Program*.

A1.24. Authority relating to providing adequate funding and personnel to establish and support an effective DoD Privacy Program; establishing and publishing Air Force-specific procedures; establishing and implementing appropriate safeguards and procedures; ensuring Air Force compliance with supplemental guidance and procedures; appointing an Air Force senior official for privacy and an Air Force privacy officer to administer the DoD Privacy Program; ensuring DoD personnel and DoD contractors having primary responsibility for implementing the DoD Privacy Program receive appropriate training; ensuring all Air Force legislative, regulatory or

other policy proposals are evaluated to ensure consistency with privacy requirements; assessing the impact of technology on the privacy of personally identifiable information (PII) and, when feasible, adopting appropriate privacy-enhancing technology; ensuring that officials who have specialized knowledge of the DoD Privacy Program periodically review AF implementation of and compliance with the DoD Privacy Program; submitting required reports; and providing required program and financial support to the Combatant Commands (CCMDs) as delegated to the Secretary of the Air Force, pursuant to DoDD 5400.11, *DoD Privacy Program*.

A1.25. Authority relating to ensuring Air Force compliance with DoD Privacy Impact Assessment (PIA) guidance and policies; establishing policies and procedures; ensuring the AF adheres to PIA requirements; and minimizing the collection and use of PII to the extent practicable as delegated to the Secretary of the Air Force, pursuant to DoDI 5400.16, *DoD Privacy Impact Assessment (PIA) Guidance*.

A1.26. Authority relating to establishing and implementing a Forms Management Program; designating a Forms Management Officer (FMO); forwarding DoD publications-related requests to the DoD FMO; designing AF forms and ensuring their accessibility for people with disabilities; approving or disapproving the creation and use of electronic versions of AF forms; ensuring prior to use that DD forms are approved for electronic use by the AF and the DoD FMO; ensuring advance testing of DoD forms used for public information collection; ensuring forms that collect personal identifying information are reviewed in accordance with DoDD 5400.11; periodically reviewing AF forms and assisting the DoD FMO in reviewing DoD forms for continued need, effectiveness, and opportunities for improvement; maintaining an inventory of approved AF forms, which identifies those approved for electronic use; ensuring appropriate life-cycle management of AF forms; using the most efficient, cost-effective methods to reproduce, store, and distribute DoD forms; and developing and distributing AF guidance for obtaining Standard Forms (SFs) and Optional Forms (OFs) as delegated to the Secretary of the Air Force, pursuant to DoDI 7750.07, *DoD Forms Management Program*.

A1.27. Authority relating to ensuring that the IT infrastructure will support enterprise, mission, functional, and Air Force Strategies; promoting and forging a strong partnership among the Air Force CIO and Comptroller, Air Force Acquisition Executive or similar position, as well as other key senior managers and external mission partners; designating, or authorizing the designation of, subordinate-level CIOs, as needed, and ensuring the subordinate CIOs have a reporting mechanism through the AF CIO; and ensuring that the Air Force's IT investment portfolio aligns with DoD Information Enterprise policies and guidance, as delegated to the Secretary of the Air Force, pursuant to DoDD 8000.01, *Management of the Department of Defense Information Enterprise*.

A1.28. Authority relating to submitting specific implementation timelines for compliance of legacy systems; ensuring new commercial wireless procurement compliance with DoD policies; ensuring all Air Force entities and entities otherwise under Air Force control that are involved in acquiring spectrum-dependent systems seek and conform to guidance from the MC4EB concerning the licensing and use of wireless systems and otherwise comply with evaluation and validation requirements; ensuring that the Authorizing Official (AO) controls wireless access to ISs, to include intrusion detection methodologies for the wireless systems; incorporating wireless topics into annual Information Assurance (IA) training; reviewing risk assessment results to make an informed risk assessment prior to granting exceptions; ensuring use of the Knowledge Management (KM) process when evaluating potential wireless solutions; and ensuring that

activities evaluating wireless technology provide feedback to the wireless KM process concerning strengths, weaknesses, vulnerabilities, mitigation techniques, and related security procedures as delegated to the Secretary of the Air Force, pursuant to DoDD 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)*.

A1.29. Authority relating to ensuring Air Force compliance with DoD Unified Capabilities (UC) policies and requirements; ensuring the Air Force provides appropriate UC to DoD and non-DoD authorized user; implementing functional requirements, performance objectives, and technical specifications for DoD networks that support UC; ensuring Air Force networks that support UC comply with approved UC Requirements (UCR) interfaces; complying with assured service features requirements; operating Air Force-owned networks that support UC with the capability to assign resources on demand, consistent with mission priorities; submitting all requests for UC transport to the Director, DISA for consideration and approval; defining and coordinating functional requirements, performance objectives, and technical specifications for DoD networks that support UC for potential inclusion in the UCR and forwarding requirements for validation and approval; planning, programming, and budgeting for UC requirements; providing read-access and limited and/or controlled write-access capabilities to Air Force-owned networks to DISA and U.S. Strategic Command (USSTRATCOM); reporting user locations to the Director, DISA; reviewing and processing all requests for waivers of UC policy and for Interim Certificates to Operate (ICTOs); and providing a representative to the DoD UC Steering Group and the DoD UC Industry Advisory Council as delegated to the Secretary of the Air Force, pursuant to DoDI 8100.04, *DoD Unified Capabilities (UC)*.

A1.30. Authority relating to supporting multi-national information sharing network projects and programs; using the Multinational Information Sharing (MNIS) network standard; and planning, programming, budgeting, and executing funding to support the MNIS Program and MNIS networks as delegated to the Secretary of the Air Force, pursuant to DoDI 8110.1, *Multinational Information Sharing Networks Implementation*.

A1.31. Authority relating to establishing an Air Force portfolio so that IT investments align to Mission Area, and sub-portfolio or capability area portfolios as appropriate; issuing guidance for managing the Air Force portfolio and designating responsibilities for Air Force portfolio management; leveraging or establishing a governance forum to oversee Air Force portfolio activities; managing the Air Force portfolio; ensuring Air Force IT investments are consistent with Mission Area, sub-portfolio or capability area portfolio guidance; and participating in Mission Area governance forums with the goal of identifying common problems in portfolio management processes and providing solutions that are in the best interest of the Enterprise as delegated to the Secretary of the Air Force, pursuant to DoDD 8115.01, *Information Technology Portfolio Management* and consistent with the provisions of DoDI 8115.02, *Information Technology Portfolio Management Implementation*.

A1.32. Authority relating to providing representatives to committees in support of Single Agency Manager (SAM) for Pentagon Information Technology Services (ITS); providing augmented and/or collocated manpower and technical expertise to the SAM for Pentagon ITS organization pursuant to support agreements, as applicable; operating and maintaining selected ITS functions and/or service centers IAW the SAM for Pentagon ITS Implementation Plan; providing estimated ITS requirements to the SAM for Pentagon ITS; assisting the SAM for Pentagon ITS in developing and executing ITS support agreements; programming, budgeting, and providing

funding for reimbursable support, support agreements, and the appropriate ITS plans, and informing the SAM for Pentagon ITS of such Pentagon ITS-related activities; coordinating, with the SAM for Pentagon ITS, those acquisitions for Pentagon IT systems, maintenance, service, or equipment to ensure compliance with the Pentagon standards-based architecture, and certifying specific ITS acquisitions IAW the SAM for Pentagon ITS Concept Plan; continuing to operate and support existing IT equipment and systems until replaced by consolidated and/or collocated facilities or until mutually agreed upon to transition responsibilities to the SAM for Pentagon ITS; and maintaining internal IT expertise, help desks, and support to user-operated office automation systems, as delegated to the Secretary of the Air Force, pursuant to DoDD 8220.1, *Single Agency Manager (SAM) for Pentagon Information Technology Services (ITS)*.

A1.33. Authority relating to ensuring information-sharing technologies and techniques curricula for stabilization and reconstruction, disaster relief, and humanitarian and civic assistance are incorporated into individual and unit training programs and Service schools; endorsing Information and Communications Technology (ICT) support requests from non-DoD entities; developing and executing an implementation plan; and establishing the procedure for validating the operational requirement of DoD-provided ICT support as delegated to the Secretary of the Air Force, pursuant to DoDI 8220.02, *Information and Communications Technology (ICT) Capabilities for Support of Stabilization and Reconstruction, Disaster Relief, and Humanitarian and Civic Assistance Operations*.

A1.34. Authority relating to implementing the Global Force Management Data Initiative (GFM DI) within the Air Force; integrating enterprise force structure data; establishing and maintaining authoritative linkages between billet-level enterprise force structure unique identifiers under the Air Force's purview and the electronic data interchange personal identifier (EDI-PI) of the individuals serving in those billets; coordinating the publication of those linkages; providing representation to GFM DI governance bodies; validating GFM DI policy and artifacts; appropriately populating and maintaining unclassified and classified organizational servers; replicating identified data in a classified Air Force server; managing investments for Air Force server development and maintenance; publishing the pedigree, security level, and access control level of Air Force server data through the applicable registries; providing Air Force server functionality pursuant to GFM DI technical guidance; exposing Military Service server data to external consumer systems; publishing the file of Air Force -specific reference data for use by data consumers; documenting and managing joint billets and joint billet organization unique identifiers (OUIDs); and supporting the transition to a force management process that enables the global sourcing of operational needs as delegated to the Secretary of the Air Force, pursuant to DoDI 8260.03, *The Global Force Management Data Initiative (GFM DI)*.

A1.35. Authority relating to ensuring all applicable initiatives, systems, services, or capabilities are consistent with DoD policy and supporting secure sharing of these assets across DoD Components and mission partners; facilitating the interoperability of data assets by ensuring DoD approved standards in acquisition and procurement are used and participating in the IT standards development process by proactively submitting change requests; ensuring the identification of pertinent governance forums and processes; funding engineering, implementation, and operation of capability demonstrations, projects, programs, initiatives, and other efforts that enable secure sharing of DoD data, information, and IT services; promoting the secure sharing of DoD data, information, and IT services and adjudicating or elevating conflicts to facilitate the secure sharing of these services; assessing resource impacts; ensuring data,

information, and IT services leverage approved enterprise identity and access management capabilities and community-accepted resource metadata tagging practices; registering required information in the Data Services Environment (DSE); implementing policies and procedures to protect data, information, and IT services while enabling their secure sharing as assets across the DoD security domains with the IC and mission partners; ensuring responsibilities and procedures for the expeditious processing of waiver requests for time-critical needs and other identified DoD policies; and coordinate with other DoD Components to identify potential enterprise data and service standards and specifications, which support interoperability as delegated to the Secretary of the Air Force, pursuant to DoDI 8320.02, *Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense*.

A1.36. Authority relating to providing an expert on Air Force operational spectrum management to support the Electromagnetic Spectrum Data community of interest (COI); providing lessons learned and feedback to the DoD Spectrum Data Administrator (DSDA); implementing procedures to ensure that all data generated at each stage of the spectrum certification process is complete, accurate, and in conformance with published spectrum-related data standards ; supporting the implementation of spectrum-related data sharing, including establishing appropriate plans, programs, recommended policies, and procedures; ensuring that all current and future spectrum-related data sharing comply with DoD policy and DSDA recommendations; designating personnel familiar with Air Force spectrum-related data to serve and perform duties as the primary contact to the DSDA; ensuring that all spectrum-dependent systems acquisitions submit spectrum-related data consistent with the Air Force's authoritative data source via the required capability; developing processes and procedures to ensure the integrity of spectrum-dependent systems data throughout their life cycle; and providing spectrum-related data requirements to the DSDA, including establishing appropriate plans, as delegated to the Secretary of the Air Force, pursuant to DoDI 8320.05, *Electromagnetic Spectrum Data Sharing*.

A1.37. Authority relating to overseeing implementation of assigned responsibilities and procedures pertaining to interoperability of information technology, including national security systems; establishing procedures for interoperability certification for IT that does not have joint, multinational, or interagency interoperability requirements; establishing procedures for reviewing Air Force IT, determining when interoperability functionality or requirements have changed, and requiring the program manager to submit that IT for interoperability recertification; designating representatives to fill identified critical roles; providing representatives to take part in and support the Interoperability Steering Group (ISG) and the Interoperability Test and Evaluation Panel (ITEP); designing, developing, testing, evaluating, and incorporating IT interoperability into all Air Force IT; requiring that all identified initial architectural views be in accordance with the current version of the DoD Architecture Framework (DoDAF); coordinating with Director, National Geospatial-Intelligence Agency, as required; and ensuring accomplishment of Air Force CIO-assigned tasks as delegated to the Secretary of the Air Force, pursuant to DoDI 8330.01, *Interoperability of Information Technology (IT), Including National Security Systems (NSS)*.

A1.38. Authority relating to requiring the use of .MIL as the primary Top Level Domain (TLD) and ensuring accomplishment of Air Force CIO-assigned tasks as delegated to the Secretary of the Air Force, pursuant to DoDI 8410.01, *Internet Domain Name Use and Approval*.

A1.39. Authority relating to executing Network Operations (NetOps) functions within Air Force-operated portions of the Global Information Grid (GIG) (now referred to as DoD Information

Networks (DoDIN)) IAW DoD policy and in support of the CCMDs responsibilities; planning, procuring, developing, testing, and implementing capabilities for operating and defending the DoDIN consistent with DoD policy and strategic guidance, ensuring doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) for operating and defending the DoDIN that are consistent with DoD policy; ensuring personnel are trained, equipped, resourced, and forces organized to implement and execute NetOps; sharing DoDIN situational awareness data with CCMDs, other DoD Components and the Intelligence Community in accordance with DoD policy; establishing and providing the necessary resources to ensure compliance with service level agreements and memorandum of agreements (MOAs) among DoDIN service providers and customers; participating in the NetOps COI; participating in identified EA efforts; and ensuring compliance with applicable DoD policies of all DoD contractors and other entities operating DoD-owned information systems and DoD-controlled information systems on behalf of the DoD that receive, process, store, display, or transmit DoD information, regardless of classification or sensitivity, as delegated to the Secretary of the Air Force pursuant to DoDI 8410.02, *NetOps for the Global Information Grid (GIG)*.

A1.40. Authority relating to executing Network Management (NM) within the Air Force portions of the Defense Information Enterprise; supporting DoD CIO, USD(AT&L), Director, DISA, and Commander, USSTRATCOM (CDRUSSTRATCOM) in developing mission-driven metrics and end-to-end NM architectures and strategies that support efficient NM operations in tactical and non-tactical networks to improve interoperability and integration across NM systems; developing strategies and architectures for IT resource management capabilities that efficiently, effectively, and securely integrate NM and spectrum management (SM) systems across DOTMLPF; supporting DISA in developing and maintaining NM standards, specifications, and interfaces to include defining extensions to baseline NM data-exchange schemas necessary to enable and facilitate the exchange and sharing of NM information and data with tactical edge NM systems; implementing common data-exchange schemas to ensure interoperability of NM systems sufficient to execute the SLAs or similar agreements; planning, organizing, procuring, developing, testing, implementing, and operating NM capabilities within established NetOps operational hierarchies and NM domain structures; supporting CDRUSSTRATCOM in establishing NetOps hierarchies that fully consider NM along with network defense and content management; supporting CDRUSSTRATCOM in developing operational requirements for automated configuration management (CM) and policy based network management (PBNM); ensuring NM systems are resilient to manmade or natural events that may cause failure, loss or disruption of NM capabilities; as needed and with DISA support, developing standard NM information and data models to include NM management information base (MIB) standards for tactical edge network elements; providing the NM and SM data necessary to fulfill the commander's critical information requirements in support of established DoD cyberspace operational hierarchies; and ensuring, in coordination with DISA, all DoD equipment containing or potentially containing personally identifiable information and other data of a sensitive nature is managed in accordance with DoDI 5000.64, as delegated to the Secretary of the Air Force, pursuant to DoDI 8410.03, *Network Management*.

A1.41. Authority relating to ensuring procurements of commercial Wireless Local-Area Networks (WLAN) products comply with DoD policy; controlling WLAN access to information systems; preparing and executing incident response plans for WLAN intrusion detection events, promoting joint interoperability through the adoption of commercial, standards-based, IA-certified WLAN products IAW DoD policy; and ensuring all users and IA managers of WLAN

devices, systems and technologies receive required training and certification; and complying with prescribed DoD procedures on WLANs as delegated to the Secretary of the Air Force, pursuant to DoDI 8420.01, *Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies*.

A1.42. Authority relating to ensuring Air Force IT complies with DoD policy; ensuring cybersecurity requirements are addressed and visible in all capability portfolios, IT life-cycle management processes, and investment programs incorporating IT; appointing an AO for all DoD Information Systems (IS) and Platform-IT (PIT) systems under the AF's purview and ensuring all DoD ISs and PIT systems are authorized; ensuring PIT systems are identified, properly designated and centrally registered at the DoD Component level; ensuring identified SSE and trusted systems and networks processes, tools, and techniques are used in the acquisition of all applicable IT under Air Force purview; ensuring that organizational solutions that support cybersecurity objectives acquired and developed via the Enterprise-wide Information Assurance and Computer Network Defense Solutions Steering Group (ESSG) process in accordance with DoD policies and guidelines are implemented when possible; participating in the ESSG process to ensure capabilities acquired or developed meet organizational requirements; providing for a cybersecurity monitoring and testing capability in accordance with DoD policy; providing for required vulnerability mitigation and incident response and reporting capabilities; ensuring that contracts and other agreements include specific requirements to provide cybersecurity for DoD information and the IT used to process that information in accordance with DoD policy; ensuring that all personnel with access to DoD IT are appropriately cleared and qualified and that access to all DoD IT processing specified types of information under Air Force purview is appropriately authorized; ensuring that personnel occupying cybersecurity positions are appropriately appointed, trained, qualified, assigned a position designation, and meet the pertinent suitability and fitness requirements; using DISA-developed cybersecurity training and awareness products and supplementing as required; ensuring that appropriate notice of privacy rights and monitoring policies are provided to all individuals accessing Air Force -owned or controlled DoD ISs; ensuring cybersecurity solutions do not unnecessarily restrict the use of assistive technology by individuals with disabilities or access to or use of information and data by individuals with disabilities; conducting vulnerability assessments and evaluations, intrusion assessments, cybersecurity inspections, and Red Team operations to provide a systemic view of enclave and IS cybersecurity posture; ensuring cybersecurity testing and evaluation is conducted throughout the acquisition life cycle and integrated with interoperability and other functional testing, and that a cybersecurity representative participates in planning, execution, and reporting of integrated test and evaluation (T&E) activities; collecting and reporting cybersecurity metrics; ensuring the required annual assessment of the Air Force cybersecurity program is conducted; using DoD guidance to develop DoD IS contingency plans and conduct exercises to recover IS services following an emergency or IS disruption; establishing a physical security program to protect DoD IT from damage, loss, theft, or unauthorized physical access; ensuring all DoD ISs under Air Force purview are registered in the appropriate DoD IT repository; ensuring all DoD IT under Air Force purview complies with applicable security technical implementation guides (STIGs), security configuration guides, and SRGs with any exceptions documented and approved by the responsible AO; establishing a cross-domain (CD) support element to coordinate CD activities with the Unified Cross Domain Management Office (UCDMO) in accordance with DoD policy and ensuring transition to using cross-domain solutions (CDSs) on the UCDMO-managed CDS

Baseline List; ensuring use of the DISA-provided CD Services as the preferred method of addressing CD requirements; implementing procedures issued by the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation (DASD(DT&E)) and Director, Operational Test and Evaluation (DOT&E) to ensure that cognizant T&E authorities for acquisition programs verify that adequate T&E support for cybersecurity requirements is planned, resourced, documented, and can be executed in a timely manner; ensuring individual and organization accountability within organizations under the Air Force purview; ensuring identified requirements on compromising emanations are funded and implemented; implementing cybersecurity and cyberspace defense capabilities responsive to DoD requirements; and ensuring that maintenance and disposal of information on DoD IT complies with DoD policies and procedures as delegated to the Secretary of the Air Force, pursuant to DoDI 8500.01, *Cybersecurity*.

A1.43. Authority relating to ensuring DoD Information Systems (IS) and PIT systems are categorized according to prescribed guidelines; verifying that a program manager (PM) or system manager (SM) is appointed for all ISs and PIT systems; ensuring a trained and qualified AO is appointed in writing for all DoD IS and PIT systems operating within or on behalf of the Air Force and that the systems are authorized in accordance with DoD policy; developing and issuing any necessary guidance for PIT systems that reflects Air Force -unique operational and environmental demands; ensuring DoD information technologies under the Air Force's authority comply with the Risk Management Framework (RMF); operating only authorized ISs and PIT systems; complying with all authorization decisions, including denial of authorization to operate (DATO), and enforce authorization termination dates (ATD); ensuring personnel engaged in or supporting the RMF are appropriately trained and possess requisite professional certifications; ensuring IS owners (ISOs) appoint user representatives (URs) for DoD IS and PIT systems under the Air Force's purview; implementing prescribed RMF policies and procedures for DoD IT; ensuring participation in the RMF TAG; and ensuring contracts and other agreements include specific requirements prescribed by DoD policy as delegated to the Secretary of the Air Force, pursuant to DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*.

A1.44. Authority relating to planning, programming, and budgeting to support the evolution of the DoD Public Key Infrastructure (PKI) program and to Public Key (PK)-Enable applicable Air Force information systems; designating offices for coordinating PKI and PK-Enabling activities; developing and implementing policies and procedures for e-mail signature and encryption using DoD-approved PKIs to support Air Force business processes; coordinating with the Director, DoD PKI Program Management Office (PMO), and the Chairman of the Joint Chiefs of Staff; establishing the Air Force portion of the infrastructure necessary to support the DoD PKI certificate life cycle and key recovery service; implementing the DoD PKI and PK-enabled information systems to use certificates for authentication, digital signatures, and encryption; PK-enabling information systems for joint programs and systems for which the Air Force is the Program Executive, Lead Agency, PMO, or equivalent; ensuring PK-enabled information systems have been tested under the PKI interoperability testing program; informing the Director, DoD PKI PMO, of information systems that have successfully completed PKI interoperability testing; coordinating with the Heads of the other DoD Components and the Director, DoD PKI PMO, for interoperability testing and PK-enabling of information systems; coordinating with the Chairman of the Joint Chiefs of Staff and the Director, DoD PKI PMO, to ensure that deployed PK-enabled information systems are capable of supporting joint-, allied-, and coalition-based

operations, as required; ensuring all DoD contracts require DoD mission partners use certificates issued by the DoD External Certification Authority (ECA) program or a DoD-approved PKI, when interacting with DoD in unclassified domains; and ensuring the Air Force provides DoD CIO with situational awareness of monitoring and compliance activities within the Air Force by reporting PKI and PK-enabling policy compliance; establishing and implementing an Air Force waiver process; submitting positively endorsed Air Force waiver requests for Defense Information System Network (DISN) Flag Panel approval, using the established Defense IA Security Accreditation Working Group (DSAWG) waiver review processes; and recommending DoD-wide waivers as required as delegated to the Secretary of the Air Force, pursuant to DoDI 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*.

A1.45. Authority relating to planning, programming, and budgeting to support the identity authentication processes for Air Force information systems and networks ensuring proper use of identity authentication processes for all Air Force information systems and networks; ensuring AF identity authentication processes are appropriately synchronized and aligned with DoD information assurance (IA) policies and privilege management initiatives; designating an office responsible for coordinating identity authentication activities across the Air Force; developing and implementing policies and procedures for use of DoD-approved public key infrastructure (PKI) certificates in PKI-based identity authentication processes for Air Force business and mission processes; and appointing AF-approved AOs to approve acceptance of risk in certification and accreditation activities in alignment with DoD policies and procedures as delegated to the Secretary of the Air Force, pursuant to DoDI 8520.03, *Identity Authentication for Information Systems*.

A1.46. Authority relating to appropriately coordinating Air Force biometrics strategies, concepts, and requirements with the DoD Biometrics Executive Committee prior to acquisition program initiation; planning, programming, and budgeting for Air Force-required biometric capabilities; ensuring that Air Force biometric training, direction, and implementation guidance is developed and implemented, as required; designating a qualified DoD Biometrics EXCOM member with required responsibilities; appropriately coordinating Air Force biometrics strategies, concepts, standards, and requirements with the DoD Biometrics EXCOM prior to program initiation or procurement actions; planning, programming, and budgeting for Air Force and, where appropriate, joint and common biometric capabilities; complying with DoD-approved policies, standards, processes, and procedures for collection, transmission, storage, archiving, caching, tagging, retrieval, and interoperation of biometric capabilities; ensuring that Air Force biometric training, direction, and implementation guidance are developed and implemented, as required; supporting geographic CCMDs; reviewing all proposed biometrics-related Air Force acquisition programs and budget submissions; and coordinating with the Biometrics PSA on such programs and submissions through Air Force participation in the DoD Biometrics EXCOM as delegated to the Secretary of the Air Force, pursuant to DoDD 8521.01, *Department of Defense Biometrics*.

A1.47. Authority relating to implementing all applicable COMSEC policies, directives, criteria, standards, and doctrine within the Air Force; reviewing and validating of all Air Force requirements for COMSEC products and services and forwarding validated COMSEC requirements to the Director, National Security Agency (DIRNSA) as necessary to support procurement activities; planning, programming, funding, implementing, managing, and providing logistics support to the COMSEC aspects of Air Force information systems; managing Air Force responsibilities of the COMSEC Material Control System (CMCS) and performing the

functions of the Service Authority; establishing and maintaining an Air Force-wide COMSEC assessment program; and developing, maintaining, and modifying Air Force -level policies, procedures, training programs, and software systems that ensure uniform application of applicable DoD policies as delegated to the Secretary of the Air Force, pursuant to DoDI 8523.01, *Communications Security (COMSEC)*.

A1.48. Authority relating to establishing Air Force Computer Network Defense (CND) Services to coordinate and direct Air Force -wide CND and ensuring system and personnel certification and accreditation in accordance with established DoD requirements and procedures; providing required operational assessments and complying with identified operational direction for the planning and conduct of CND and the integration of IA activities into CND operations; complying with identified reporting requirements; providing operational requirements and priorities, operational status and the user's perspective on computer network status; maintaining an inventory that is available to required users/reviewers; managing specified designations and assignments; ensuring CND Services (CNDS) support is a condition of information and computer system IT security certification and accreditation; providing guidance on certain service arrangements; developing a coordinated and common DoD curriculum for CND education, training and awareness; participating in planning and establishing Air Force requirements for a Defense-wide common operating picture; planning, programming and monitoring Air Force -assigned responsibilities for development of information systems or databases supporting Defense-wide CND; establishing Air Force sensor grid requirements and planning and programming for their implementation; coordinating system development and integration; and supporting CND Architect sponsored activities and responding to requests for information as delegated to the Secretary of the Air Force pursuant to DoDI O-8530.2, *Support to Computer Network Defense (CND)*, marked as FOUO.

A1.49. Authority relating to the Air Force's responsible operation of DoD Internet services and use of Internet-Based Capabilities (IbC) in compliance with DoD policies; disseminating DoD information via DoD Internet services and IbC; educating and training subordinate DoD employees in the responsible and effective use of DoD Internet services and IbC; and ensuring all DoD Internet services and IbC used by the Air Force to disseminate unclassified DoD information are assessed at least annually for compliance as delegated to the Secretary of the Air Force, pursuant to DoDI 8550.01, *DoD Internet Services and Internet-Based Capabilities*.

A1.50. Authority relating to designating in writing a qualified primary and one or more qualified alternate voting representatives to the Ports, Protocols, and Services (PPS) Management (PPSM) CCB chairperson and ensuring representation at all PPSM CCB meetings; providing guidance and overseeing Air Force DoD IT implementations including information systems, PIT systems, PIT, and products to ensure PPS are properly used, assessed, declared, implemented, regulated, verified, documented and approved in compliance with DoD policy; assuring the interoperability of DoD IT in accordance with applicable DoD policies and processes; submitting exception requests; initiating the approval process for identified uses of PPS; and overseeing identified Air Force uses of PPS as delegated to the Secretary of the Air Force, pursuant to DoDI 8551.01, *Ports, Protocols, and Services Management (PPSM)*.

A1.51. Authority relating to establishing, resourcing, and implementing cybersecurity training and certification programs for all Air Force personnel; providing initial IA awareness orientation and annual IA refresher awareness to authorized users; identifying, documenting, and tracking IA personnel certifications and certification status in Air Force personnel databases; identifying

military IA billets in manpower databases based on operational mission support and force structure requirements; ensuring that all DoD civilian positions and personnel regardless of Office of Personnel Management (OPM) series or job title, with IA functions use "INFOSEC" as the Position Specialty Code (PSC) in the Defense Civilian Personnel Data System; requiring contracts that include the acquisition of DoD IS IA services to specify certification requirements and requiring contractor personnel performing IA functions to have their IA certification category and level documented in the Defense Eligibility Enrollment Reporting System; identifying, documenting, tracking, and reporting to the DoD CIO the certifications and certification status of all contractors performing privileged user or IA manager functions; requiring all AOs to be certified; providing appropriate IA training for required personnel; providing CND training to CND staffs; including IA awareness training and education, as appropriate, in professional military education at all levels; capturing and reporting the costs of IA training and certification of personnel; and encouraging the use of the Information Assurance Scholarship Program to recruit, develop, and retain DoD IA personnel as delegated to the Secretary of the Air Force, pursuant to DoDD 8570.01, *Information Assurance Training, Certification, and Workforce Management*.

A1.52. Authority relating to ensuring cybersecurity is implemented in all system and service acquisitions in accordance with issued USD (AT&L) guidance; establishing and implementing internal management processes for the preparation and review of Acquisition IA Strategies; designating a principal point of contact to represent the Air Force on policy and procedural matters regarding IA in the acquisition system; and establishing and implementing procedures for the submission and review of Acquisition IA Strategies as delegated to the Secretary of the Air Force, pursuant to DoDI 8580.1, *Information Assurance (IA) in the Defense Acquisition System*.

A1.53. Authority relating to ensuring space systems compliance; ensuring that solicitations, contracts, or formal agreements executed by the Air Force to acquire space systems from commercial, other USG, or foreign government-owned entities require compliance with identified instructions and regulations; coordinating with the DIRNSA, in developing appropriate cybersecurity-related language for identified solicitations, contracts, or formal agreements; ensuring program managers for space systems under the Air Force's responsibility include information system security engineering (ISSE), crypto certification, and certification and accreditation (C&A) in their program plans, budgets, and contracts, as appropriate; and ensuring the validation of IA requirements for space systems that do not support joint and combined operations through appropriate requirement oversight authorities as delegated to the Secretary of the Air Force, pursuant to DoDI 8581.01, *Information Assurance (IA) Policy for Space Systems Used by the Department of Defense*.

A1.54. Authority relating to ensuring unclassified DoD information provided to or developed by non-DoD entities is minimally protected by including requirements implementing DoD policy in contracts, grants, and other legal agreements; ensuring additional protection measures or reporting requirements regarding compromise, loss, or unauthorized disclosure required by DoD policies are implemented by the insertion of applicable requirements into contracts, grants, and other legal agreements; and ensuring that contracts include appropriate Defense Federal Acquisition Regulation Supplement (DFARS) clauses for safeguarding unclassified DoD information on non-DoD information systems as delegated to the Secretary of the Air Force,

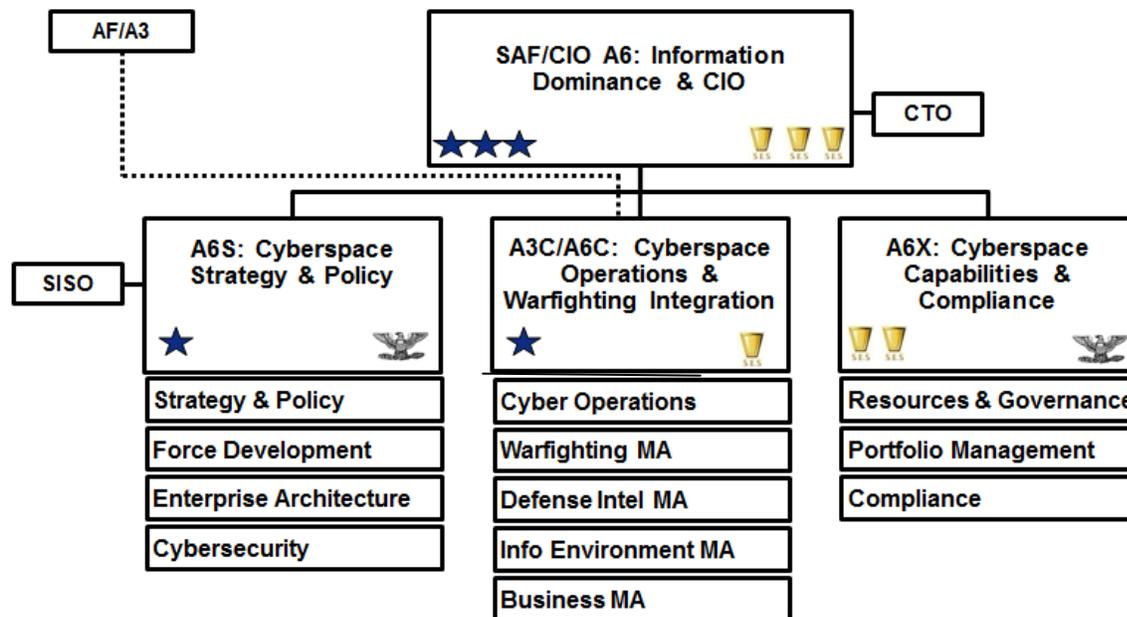
pursuant to DoDI 8582.01, *Security of Unclassified DoD Information on Non-DoD Information Systems*.

A1.55. Authority relating to responding only to identified information collections; collecting information consistent with OMB requirements; ensuring that users justify new information collection requirements and that data is not available from other sources, duplicated or unnecessarily generated; determine whether information collected is releasable to other Federal agencies; establishing an information collections control activity; establishing goals to reduce the number or frequency of internally prescribed information collections; and ensuring the Air Force assesses its information collections for necessity and cancels unnecessary information collections or modifies the information collection to reduce burden as delegated to the Secretary of the Air Force, pursuant to DoDI 8910.01, *Information Collection and Reporting*.

A1.56 Authority relating to appointing or designating a senior agency information security officer, developing and maintaining an agency-wide information security program, developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities, assisting senior agency officials concerning identified responsibilities, and otherwise complying with Air Force responsibilities assigned to the Secretary of the Air Force pursuant to 44 USC § 3544, *Federal Agency Responsibilities*.

ATTACHMENT 2

**CHIEF, INFORMATION DOMINANCE AND
CHIEF INFORMATION OFFICER
(SAF/CIO A6)**



A2.1. The Chief, Information Dominance and Chief Information Officer, (SAF/CIO A6) is responsible for cyberspace/Information Technology (IT) policies and concepts; command and control (C2); cyberspace operations; enterprise-wide integration of Air Force cyberspace/IT, including National Security Systems (NSS); information resources management (IRM); spectrum management; information systems; cybersecurity; information management (IM); knowledge management (KM); postal operations; warfighting integration; and related matters for the Department of the Air Force, pursuant to 40 USC § chapter 113, subchapter III. The SAF/CIO A6 also serves as the Department of the Air Force Enterprise-level strategist and business advisor from the cyberspace/IT, and IRM perspective; Information and IT architect for the Department of the Air Force enterprise; and, Air Force-wide cyberspace/IT and IRM executive. The Secretary of the Air Force retains ultimate responsibility for all policies related to the Department of the Air Force. Within his/her areas of responsibility, the SAF/CIO A6 prepares policies for approval and issues official guidance/procedures via official Department of the Air Force publications to ensure implementation of those policies.

A2.1.1. Senior Information Security Officer (SISO): The SISO is appointed by the Air Force CIO to carry out his/her responsibilities under DoDIs 8500.01 and 8510.01. These duties include the following: establish and enforce the Air Force's cybersecurity program; establish Air Force cybersecurity and Assess and Authorization policies; develop and issue guidance for PIT systems that reflect Air Force unique demands, function as Security Control

Assessor (SCA) or formally delegates SCA for all Air Force systems; ensure compliance with DoD Risk Management Framework (RMF); appoint system, function or mission Authorizing Officials for SecAF; appoint primary and alternate members of RMF Technical Advisory Group (TAG); and appoint chairs to Air Force RMF Process TAG.

A2.1.2. Chief Technology Officer (CTO): The CTO advises the Air Force CIO on cyberspace/IT emerging technology, enterprise architecture, enterprise infrastructure, and strategy including identifying short- and long-term goals of Department-wide cyberspace/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 and Major Commands (MAJCOMs) on cyberspace/IT issues, activities and impacts.

A2.2. Subordinate organizations/offices include:

A2.2.1. Cyberspace Operations and Warfighting Integration Directorate

(AF/A3C/A6C). The Air Force CIO shares operational control of AF/A3C/A6C in the role of the Air Force CIO's single manager for cyberspace operations and integration across mission areas. AF/A3 shares operational control of AF/A3C/A6C with SAF/CIO A6 in the role of the Air Force's managers for cyberspace operations. SAF/CIO A6 has administrative control of the AF/A3C/A6C staff activity. AF/A3C/A6C develops concepts of operations (CONOPS) and resource roadmaps to enable Air Force forces to generate, project, and sustain a single integrated information domain and provide cyberspace capabilities to enhance Air Force core missions in air, space, and cyberspace. AF/A3C/A6C serves as the Mission Area Integration Lead responsible for synchronizing warfighting IT/NSS priorities with SAF/CIO A6 strategic direction within the DoD defined mission areas of business (BMA), information environment (IEMA), defense portion of intelligence (DIMA), and warfighter (WMA).

A2.2.2. Cyberspace Policy and Strategy Directorate (SAF/CIO A6S). SAF/CIO A6S develops plans, policy and guidelines for and provides oversight of the processes and procedures to integrate warfighting and combat support capabilities and the implementation of enterprise command and control, warfighter networking, and combat support data management capabilities for Joint, Coalition, and Air Force warfighters. It develops and maintains the Air Force Information Dominance Flight Plan. SAF/CIO A6S accommodates all approved C2 and space strategic goals by integrating them into the Air Force Information Dominance Flight Plan and inform the Air Force Strategic Master Plan. SAF/A6S serves as the cyberspace functional manager, leading the development and delivery of forces in coordination with AF/A2 to meet Service and combatant commander requirements through workforce development, strategic planning and contingency operations. SAF/A6S supports the Air Force Strategic Planning Process and ensures SAF/CIO A6 priorities, policies, guidance and activities align with the OSD and Air Force Strategic plans. SAF/A6S provides oversight and guidance to enable the development of the total Cyberspace Operations force from the start of a career to the end of a career. SAF/CIO A6S serves as the Functional Manager for the 17D, 17S, 1B, 3D and 3A Air Force Specialty Codes (AFSCs) and related civilian career fields. It develops, coordinates, publishes, implements, and enforces guidelines and procedures for network/system assessment and authorization. It oversees policy and guidance for cybersecurity for the Air Force, ensures cybersecurity requirements

are addressed and visible in all capability portfolios, and ensures cybersecurity testing and evaluation is conducted throughout the acquisition life cycle. It represents the SAF/CIO A6 as the Senior Information Security Official for the Air Force. It provides support to the SAF/CIO A6 in the assessment of technology and industry trends to shape the development of policies and procedures standards and architectures which guide Air Force cyberspace/IT investments. By SAF/CIO A6 appointment, the Director serves as the Air Force Chief Architect and manages the Air Force EA process. SAF/CIO A6S supports the Air Force Strategic Planning Process and ensures SAF/CIO A6 priorities, policies and activities align with the Air Force Strategic Master Plan.

A2.2.3. Cyberspace Capabilities and Compliance Directorate (SAF/CIO A6X). SAF/CIO A6X develops the policy and guidance and provides oversight for the processes and procedures associated with Information Technology (IT) Governance across the Air Force. SAF/CIO A6X manages the Air Force IT Portfolio Management process. It monitors compliance with Air Force and OSD policy and guidance, congressional mandates and legal obligations such as IT certification and registration and the Clinger-Cohen Act. SAF/CIO A6X develops and manages the CIO Governance and Compliance frameworks in support of the SAF/CIO A6 mission. SAF/CIO A6X leads development and reporting of the Air Force Cyberspace/IT Budget. SAF/CIO A6X validates requirements for cyberspace operational capabilities. SAF/CIO A6X manages and coordinates SAF/CIO A6 equities in the Air Force requirements process and in Joint Capabilities Integration and Development System (JCIDS).

ATTACHMENT 3

STANDARD OPERATING PROCEDURES

BETWEEN THE

AIR FORCE CHIEF, INFORMATION DOMINANCE AND

CHIEF INFORMATION OFFICER (SAF/CIO A6)

AND THE

AIR FORCE CHIEF OF SAFETY (AF/SE)

These standard operating procedures (SOPs) apply to individuals assigned to the Chief, Information Dominance and Chief Information Officer (SAF/CIO A6) and Air Force Chief of Safety (AF/SE) who are responsible for developing policy, managing programs, and preparing guidance on approved policies and plans concerning munitions certification authority for Hazards of Electromagnetic Radiation to Ordnance (HERO). These procedures are intended to facilitate routine staff actions and functions and reduce duplication of effort between SAF/CIO A6 and AF/SE staff roles while increasing operating effectiveness and efficiency.

A3.1. SAF /CIO A6 retains authority and responsibility for the Air Force Electromagnetic Environment Effects (E3) program and Hazards of Electromagnetic Radiation to Ordnance (HERO), as it relates to E3, as delegated through public law, executive order or Department of Defense Directives (DoDD) and Instruction (DoDI) including DoDD 3222.3. AF/SE retains authority and responsibility for safety and nuclear surety as delegated or re-delegated through public law, executive order or Department of Defense Directive and Instruction.

A3.2. Subject to the standard operating procedures that follow, a general description of the flow of work between AF/SE and SAF/CIO A6 for the specific programs described in A5.1 is:

A3.2.1. SAF/CIO A6 submits E3 policies that impact HERO certification to AF/SE for coordination and concurrence prior to publication.

A3.2.2. AF/SE submits HERO policies that impact the E3 program to SAF/CIO A6 for coordination and concurrence prior to publication.

A3.2.3. AF/SE executes HERO certification authority for munitions tested in accordance with DoD Standard 6055.09-STD, during acquisition and subsequent phases of life-cycle management.

A3.3. **Conditions Requiring AF/SE Review of SAF/CIO A6 Actions.** AF/SE review and concurrence are required prior to implementing any policy, plan, and program which involves HERO.

A3.4. **Conditions Requiring SAF/CIO A6 Review of AF/SE Actions.** SAF/CIO A6 review and concurrence are required prior to implementing any policy, plan, and program which involves the management or execution of the Air Force E3 program to include HERO.

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/CIO A6 or AF/SE may also initiate a revision. OPRs must follow revision procedures as mandated in HOI 90-1, Headquarters Air Force Mission Directives – Delegations of Statutory Authority and Assignment of Responsibilities.

//signed, kfn, 20 Sep 13//
KURT F. NEUBAUER
Major General, USAF
Chief of Safety

//signed, mjb, 20 Sep 13//
MICHAEL J. BASLA
Lieutenant General, USAF
Chief, Information Dominance
and Chief Information Officer