BY ORDER OF THE COMMANDER
AIR FORCE RESERVE COMMAND

AIR FORCE RESERVE COMMAND
INSTRUCTION 17-101

29 MAY 2019

Cyberspace

AIR FORCE RESERVE CHIEF INFORMATION OFFICER (CIO) GOVERNANCE STRUCTURE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing web site at **http://www.e-publishing.af.mil/**

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: HQ AFRC/A6XC

Certified by: HQ AFRC/A6X
(Fred L. Massey, GS-14)

Supersedes: AFRCI 33-101, 25 April 2012

Pages: 22

This instruction implements AFPD 17-1, *Information Dominance Governance and Management*, and references AFPD 17-2, *Cyberspace Operations*. It codifies April 2017 AFRC/CC approval of the Air Force Reserve (AFR) Chief Information Officer (CIO) governance structure to be used for implementing CIO responsibilities within AFR to promote the most effective and efficient application, acquisition and management of information technology resources throughout the command. This instruction serves as the overarching charter for the CIO governance structure and the listed CIO-related boards and working groups. This instruction applies to Headquarters Air Force Reserve Command (HQ AFRC), all AFRC Numbered Air Forces (NAFs), AF/RE, Headquarters Air Reserve Personnel Center (HQ ARPC), and all AFR units. This instruction does not apply to Regular Air Force or Air National Guard (ANG) organizations. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). Send recommended changes or comments to the Office of Primary Responsibility (OPR), Headquarters Air Force Reserve, Communications and Information Directorate, Plans and Programs Division, CIO Support Branch (HQ AFRC/A6XC), 155 Richard Ray Blvd, Robins Air Force Base (AFB), GA 31098, using AF Form 847, *Recommendation for Change of Publication*. This publication may be supplemented at any level, but all Supplements must be routed to the OPR of this publication for coordination prior to certification and approval. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See AFI 33-360, *Publications and Forms*

Management, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the Publication OPR for non-tiered compliance items.

SUMMARY OF CHANGES

This document has been substantially revised and needs to be completely reviewed. Major changes include: expands the AFRC/A6 CIO role to the Career Field Manager (CFM); aligns the Chief Technology Officer (CTO) role underneath the CIO; incorporates the AFR Chief Data Officer (CDO) and Chief Enterprise Architect (CEA) responsibilities into A6 with direct oversight of all AFR business systems; shifts from a decision-making CIO Board to a CIO Advisory Committee to more directly empower the CIO; splits configuration control for infrastructure and AFR business systems from a singular Enterprise Configuration Control Board (ECCB) into two separate configuration control boards; and removes domain leads.

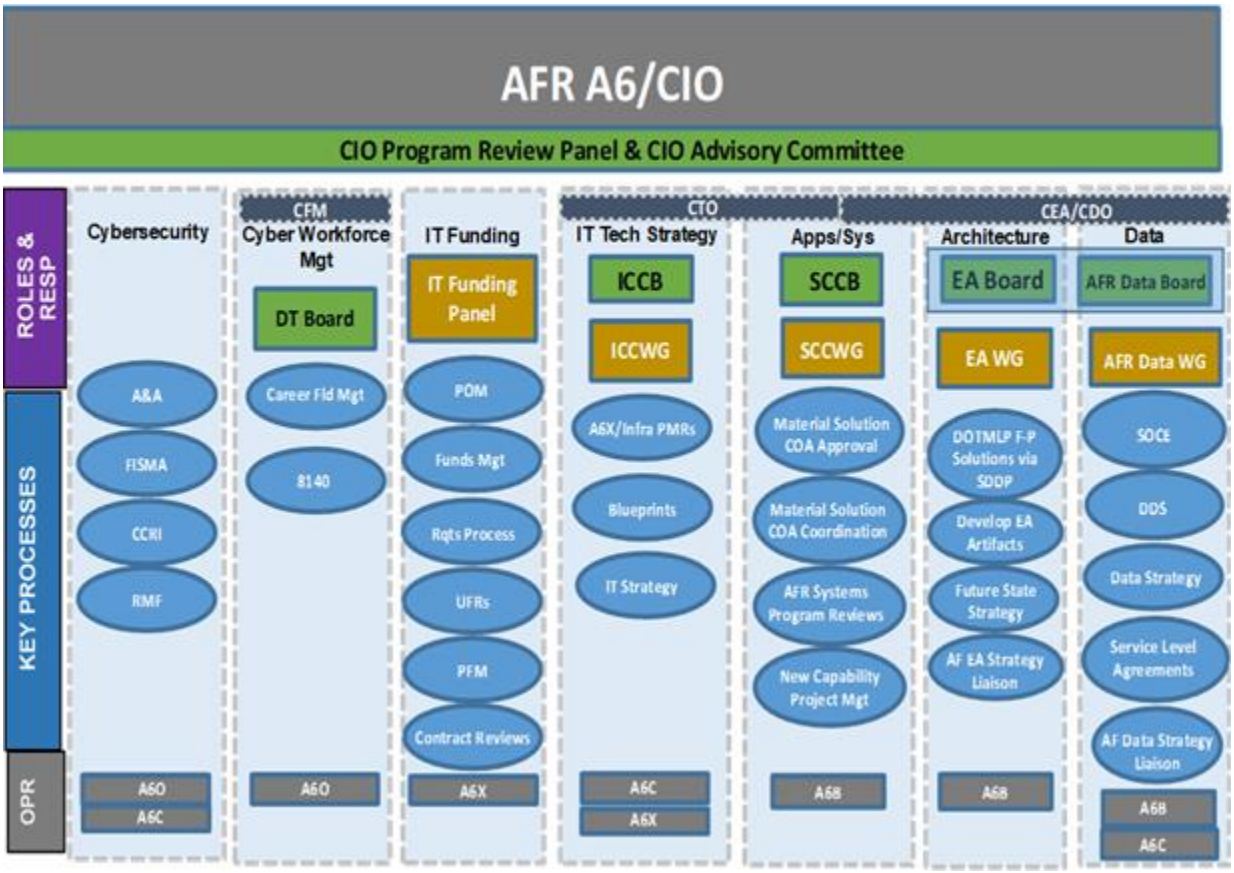
1. CIO Background. The Information Technology Management Reform Act (ITMRA) of 1996 (aka, the Clinger-Cohen Act) established the role of the CIO to improve the acquisition and use of Information Technology (IT) in support of strategic mission performance. Specific CIO responsibilities include IT acquisition, capital planning and investment, cybersecurity, e-Gov/e-Business, enterprise architecture, enterprise information management, leadership/management, performance and results-based management, policy, process improvement, project/program management, strategic planning, and technology assessment.

2. AFR CIO Scope. HQ AFRC/A6 has primary responsibility for Cybersecurity, Cyber Workforce Management, IT Funding, IT Tech Strategy, Applications and Systems, Architecture and Data. These CIO responsibilities encompass the entire AFR, to include HQ AFRC and special staff, AF/RE, ARPC, NAFs, and all AFR units.

3. AFR CIO Governance Structure. AFR utilizes a hierarchal CIO governance structure, incorporating a number of boards, working groups, and teams focused on specific CIO areas of responsibility (Fig 1). This ensures that appropriate AFR-wide input and perspective is provided

on CIO-related activities and decisions. While these groups are distinct, their supporting processes, decisions and other outputs are inter-related and inter-dependent. Its purpose is to achieve the overarching CIO goal of ensuring effective, efficient, and compliant use of IT resources to meet AFR mission needs. All AFR organizations are responsible for ensuring the AFR CIO is included in any governance decisions (including Total Force) related to AFR IT enabling capabilities and AFR business systems.

Figure 1. AFR CIO Governance Structure.



4. AFR CIO Governance Roles and Responsibilities.

4.1. **AFR Chief Information Officer (CIO).** The Director of Communications, Headquarters AFRC (HQ AFRC/A6), is designated as AFR CIO. The AFR CIO serves as the Reserve focal point for assuring all IT–related planning, management, investment, evaluation, and revalidation efforts are meeting the Reserve's operational and business objectives and adhering to AF-CIO and Clinger-Cohen directives. As AFR CIO, HQ AFRC/A6 provides oversight on issues related to cybersecurity, cyber workforce management, IT funding, IT infrastructure and technology strategy, AFR applications/systems, AFR enterprise architecture and AFR data. Specific CIO responsibilities include:

4.1.1. Serves as SAF/CIO A6's designated subordinate AF CIO to work across AFR in consolidating, developing, interpreting, disseminating, and executing AF CIO guidance in accordance with established Headquarters Air Force (HAF) overarching policy.

4.1.2. Establishes and manages strategies, policy, procedures, and standards related to the management and oversight of AFR IT.

4.1.3. Oversees the AFR IT portfolio, to include IT funding management, assessment and evaluation of AFR IT programs.

4.1.4. Provides oversight and management of network operations and the communications and computing transport layer.

4.1.5. Provides, executes, and enforces Cyber Security policy, guidelines, and procedures for the AFR, including the development and sustainment of an information security program.

4.1.6. Develops and approves IT performance measures.

4.1.7. Advises on IT matters related to strategic planning, readiness, and modernization.

4.1.8. Establishes panels, working groups, etc. as needed to focus on specific CIO areas of interest.

4.1.9. Reviews and approves issues elevated from subordinate CIO groups.

4.1.10. Elevates key IT issues for AFR Corporate Structure decision when necessary.

4.1.11. Determines when IT issues warrant AFR CIO Advisory Committee and/or AFRC Corporate Structure review.

4.1.12. Chairs AFR CIO Advisory Committee and AFR Program Review Panel.

4.2. **AFR Deputy Chief Information Officer (A6D).** The Executive Director of Communications, Headquarters AFRC (HQ AFRC/A6D), is designated as AFR Deputy CIO. In the absence of the CIO, the Deputy CIO carries out the CIO responsibilities as outlined in paragraph **4.1**. Specific responsibilities include:

4.2.1. Member of CIO Program Review Panel.

4.2.2. Chairs the AFR IT Infrastructure Configuration Control Board (ICCB).

4.2.3. Chairs the System/Application Configuration Control Board (SCCB).

4.2.4. Chairs the Enterprise Architecture Board (EAB)/Data Board.

4.3. **AFR Chief Technology Officer (CTO).** The AFR CTO is responsible to the AFRC/A6 CIO to ensure efficient and effective use of AFR IT and cyber resources for mission assured capabilities. The AFR CTO serves as the Reserve focal point for assuring all IT/NSS (Information Technology/Network Security Services) architecture–related planning, management, investment, evaluation, and revalidation efforts are meeting the Reserve's operational and business objectives and adhering to AF-CIO and Clinger-Cohen directives. Specific CTO responsibilities include:

4.3.1. Oversees IT tech strategy.

4.3.2. Collaborates with AFR CEA/CDO to oversee AFR business systems and applications.

4.3.3. Special advisor to the ICCB, SCCB, EA/Data Boards.

4.3.4. Attends Working Groups as needed.

4.4. **Chief Enterprise Architecture (CEA).** The AFR Chief Enterprise Architect (CEA) leads the effort to develop, maintain, govern, and evolve AFR enterprise architecture. The AFR CEA works directly for the AFRC/A6 Chief Information Officer (CIO) overseeing the AFR Enterprise Architecture (EA) team. Specific CEA responsibilities include:

4.4.1. Key advisor to the AFR EAB.

4.4.2. Provides technical and strategic architecture assistance to the AFR CIO and CTO.

4.4.3. Integrates AF/RE, AFRC, and ARPC EA activities.

4.4.4. Provide guidance and oversight for all AFR EA activities.

4.4.5. Determine AFR architecture to be forwarded to Air Force Enterprise Architecture for incorporation into the Air Force Enterprise Architecture (AFEA).

4.4.6. Support in the development of AFR CIO governance and drive program strategy.

4.4.7. Advises on EA matters related to strategic planning, readiness, and modernization

4.4.8. Assist functional experts and AFR Unique Business Application Managers in developing operational and systems architectures.

4.4.9. Advocate AFR unique requirements to AF functional domain owners for integration into AF and DoD solutions.

4.4.10. In conjunction with AFR CTO, reviews AFR-unique business systems, applications, capabilities and proposes transition plans.

4.4.11. Provides EA recommendations for approval.

4.4.12. Provides architectural advice and proposes tech solutions as requested.

4.4.13. Supports AFR Portfolio Management and Requirements Management efforts.

4.4.14. Manages AFR architecture review process.

4.4.15. Attends functional working groups/board meetings to assist with the development of required architecture artifacts prior to the deployment of sustainment or enhancement capabilities.

4.4.16. Establishes and manages strategy, policies, procedures, and standards to govern enterprise architecture, Service Orientated Architecture and business systems within AFR.

4.4.17. Utilizes architecture checklist to determine when sustainment artifacts (used for NDAA and Clinger Cohen Act compliance) are necessary and which types of artifacts are required for enhancements.

4.4.18. Support the development of all required AF & Department of Defense (DoD) artifacts required for certification.

4.4.19. Ensures alignment of AFR efforts to AF strategies, policies, procedures, and standards.

4.4.20. Serves as an outward facing conduit between AFR and external orgs to represent AFR business system interests and enterprise architecture interests, to include interfacing with AF Functional CIOs, coordinating software development-related requirements as

necessary through appropriate AF governance structures and advocating for integration of AFR requirements into AF, DoD, or other Federal systems where possible.

4.4.21. Assists functional experts in developing operational and systems architectures and strategies to meet AFR unique requirements that ensure enterprise information technology solutions are utilized effectively and efficiently.

4.4.22. Provide technical recommendations for new initiatives and enhancements to existing capabilities.

4.4.23. Implements modernized information exchanges to replace legacy point to point interfaces with service oriented architecture based technology.

4.4.24. Approves Enterprise Architectures and related measures.

4.4.25. Key Advisor to the AFR SCCB to ensure data, architecture, and migration path aspects are factored into AFR system decisions.

4.4.26. Promotes AFR Business Process Reengineering (BPR) initiatives related to IT.

4.4.27. Carries out EA Program objectives. (See **Attachment 2**).

4.5. **Chief Data Officer (CDO).** The CDO provides guidance and direction on how the organization will govern and manage data and Data Management systems to improve organizational efficiency and effectiveness. The AFR CDO works directly for the AFRC/A6 Chief Information Officer (CIO). Specific responsibilities include:

4.5.1. Key advisor to the AFR Data Board.

4.5.2. Provides technical and strategic data management assistance to the AFR CIO and CTO.

4.5.3. Establishes and manages strategy, policies, procedures, and standards to govern data management access within AFR.

4.5.4. Ensures alignment of AFR data efforts to AFR EA and AF strategies, policies, procedures, and standards.

4.5.5. Serves as an outward facing conduit between AFR, internal and external orgs to represent AFR data management interests.

4.5.6. Leads digital transformation to data-driven culture within AFR that utilizes data as a strategic corporate asset to meet business needs.

4.5.7. Provides oversight of creation, capture, collection, use, analysis, management, maintenance, sharing, and storage of data within AFR.

4.5.8. Develops/maintains partnerships with AFR Functional Organizations, AF IDB/C, AF, Functional CIO’s, SAF/ESWG.

4.5.9. Acts as liaison to the AF for AF data strategy and data related issues.

4.5.10. Represent Reserve Component and AFRC MAJCOM enterprise data interests to the Air Force Data Panel (AFDP).

4.5.11. Implements the AF Enterprise Data Management Program at the organizational level.

4.5.12. Validates and approves AFR Authoritative Data Sources (ADS) submissions to AF

4.5.13. Defines minimum AFR standards for data.

4.5.14. Stands up COIs as needed to support new data requests, requirements, and capabilities.

4.5.15. Reviews Information Asset requests for establishment or coordination with AF Chief Data Office or Mission Area, as applicable.

4.5.16. Adjudicates ADS access denials within its organization and elevates to AF CDO when appropriate, including request for external data.

4.5.17. Reviews and approves data policies, standards, metrics, and procedures.

4.5.18. Reviews and approves data architecture, data models, and specifications.

4.5.19. Sponsors and oversees Data Management projects and services.

4.5.20. Monitors and enforces data policies and practices within the organization.

4.5.21. Produces and/or identifies data sharing education and Data Management strategies.

4.5.22. Oversees execution of the enterprise data strategy.

4.5.23. Works with CIO management to implement the cross-functional data sharing.

4.5.24. Carries out Data Program objectives. (See **Attachment 3**)

4.6. **AFR CIO Advisory Committee.** The purpose of the CIO Advisory Committee is to provide a corporate forum for overarching cross-functional advisory support for CIO-related responsibilities, to include IT policies, IT modernization efforts, IT requirements, IT funding, AFR Systems, CIO compliance issues, Architectures, IT Training Strategies, and CIO performance measures. Committee members will provide the perspective of their area of responsibility for CIO-related issues, decisions, and strategies, and will be responsible for ensuring implementation of AFR CIO-related IT, architecture, data, and systems policies and decisions within their area of responsibility. The following are designated as AFR representatives and the frequency of this meeting:

4.6.1. Chair: AFR CIO.

4.6.2. Secretariat: HQ AFRC/A6XC.

4.6.3. Members: All HQ 2-letter Directors and equivalent Special Staff and O-6-equivalent representatives appointed from AF/RE, ARPC, and NAFs. Additional members may be added at the discretion of the AFR CIO. (Note: Remote participation will be available for AFR CIO Advisory Committee participants not located at Robins AFB).

4.6.4. Meetings: Twice per year at a minimum; additionally at discretion of AFR CIO. Semi-annual updates to Directors-only meeting will also be used to provide CIO topic awareness, as appropriate. Combined Staff Meeting can be leveraged to share immediate CIO info as appropriate.

4.7. **AFR CIO Program Review Panel.** The purpose of the CIO Program Review Panel is to ensure AFR CIO, as the SAF CIO-designated subordinate CIO, has oversight and influence on all AFR IT investment decisions and the ability to direct Information Environment capabilities. The Program Review Panel will annually review (at a minimum) all infrastructure and business system programs/investments in the AFR IT portfolio, encompassing integrated review of financial, technical, contract, cyber security, performance, and architectural issues. Other AFR CIO boards/groups and A6 division leads may determine other topics to be elevated for CIO awareness/input via the Program Review Panel. The following are designated as AFR representatives and the frequency of this meeting:

4.7.1. Chair: AFR CIO.

4.7.2. Secretariat: HQ AFRC/A6X.

4.7.3. Members: HQ AFRC/A6D, HQ AFRC/A6 Div Chiefs, HQ AFRC/A6XR, HQ AFRC/A6XC, HQ AFRC/A6OS (Cybersecurity). HQ Directors, and others will participate as briefing content dictates.

4.7.4. Meetings: Weekly.

4.8. **Developmental Team Board (DT).** The purpose of the Developmental Team Board is to provide a structured manner to develop our AFR cyber officer and enlisted members to support mission capabilities. The DT evaluates member records annually to provide deliberate guidance maximizing individual goals and potential through vectors or career counseling. The Reserve-Development Plan (R-DP) is the avenue in which reservists communicate their desire for development. The DTs use the R-DP to link the Airman's desires, potential leadership, education, training, and experience with the needs of the AFR. The following are designated as AFR representatives and the frequency of this meeting:

4.8.1. Chair: HQ AFRC/A6 (Career Field Manager).

4.8.2. Secretariat: HQ AFRC/A6OD.

4.8.3. Members: A6 will select General Officers, Colonels and senior enlisted personnel (Enlisted DTs only) throughout the career field serving in different reserve statuses to serve as board members.

4.8.4. Meetings: Annually at HQ ARPC

4.9. **AFR IT Funding Panel.** The purpose of the AFR IT Funding Board is to provide Action Officer-level (AO) cross functional input on IT funding strategies and IT requirements prioritization, as well as other CIO-related reviews as directed. The IT Funding Board will provide technical, operational, and tactical assessments in support of AFR IT funding issues, oversee the financial aspects of the IT portfolio, and recommend a prioritized unfunded IT requirements list for submission to the AFR CIO. The following are designated as AFR representatives and the frequency of this meeting:

4.9.1. Chair: HQ AFRC/A6X.

4.9.2. Secretariat: HQ AFRC/A6XC.

4.9.3. Members: Designated representatives from all HQ AFRC 2-letter orgs, HQ AFRC/A6 divisions, RE, Force Generation Center (FGC), ARPC, and NAFs. Those who

submit requirements and/or have a stake in content being briefed also will be invited to participate as appropriate.

4.9.4. Meetings: Quarterly at a minimum; additionally at discretion of chair. Meetings should precede Financial Management Working Group (FMWG), Agile Combat Support (ACS) panel reviews, etc. if possible. (Note: Remote participation will be provided for members not located at Robins AFB.).

4.10. AFR IT Infrastructure Configuration Control Board (ICCB). The purpose of the ICCB is to:

4.10.1. Authorize/approve the establishment of Enterprise baselines.

4.10.2. Authorize additions/deletions/modifications of items to/from baseline.

4.10.3. Represent the interests of all groups who may be affected by changes to the baselines.

4.10.4. Evaluate and approve, disapprove, or defer proposed Enterprise changes.

4.10.5. Modify and approve timelines for Enterprise enhancements and changes to the baseline.

4.10.6. Coordinate implementation of approved changes.

4.10.7. Resolve adverse impact of changes

4.10.8. The ICCB is responsible for authorizing baselines; reviewing and approving additions, deletions, or modifications to baselines; evaluating, approving/disapproving, and prioritizing change requests impacting system configurations; approving infrastructure-related roadmaps and tech refresh strategies; and overseeing infrastructure-related Program Management Reviews (PMRs). The following are designated as AFR representatives and the frequency of this meeting:

4.10.8.1. Chair: Deputy CIO.

4.10.8.2. Secretariat: HQ AFRC/A6C.

4.10.8.3. Members: CTO, CEA/CDO, A6X, Federal Information Systems Management Act (FISMA) Accrediting Systems Information Security Officers (ISOs), Information Systems Security Managers (ISSMs) and Information System Security Officers (ISSOs) , Enterprise Configuration Manager (A6CO), HQ AFRC ISSM (A6CO), Enterprise Architecture, Organizational (ISSO) (A6CN), Cybersecurity, (A6OS), Organizational Cybersecurity Liaisons, Functional Mission Partners (e.g. A3), AFR Business Systems (e.g. FM for AROWS-R), Vendor Mission Partners, User Representatives.

4.10.8.4. Meetings: Quarterly at a minimum; additionally at discretion of chair.

4.11. **AFR IT Infrastructure Configuration Control Working Group (ICCWG).** The purpose of the ICCWG is to provide AO-level input and review of configuration management issues for the lifecycle of enterprise IT infrastructure programs, to include network, Video Teleconference (VTC), voice, radios, etc. The ICCWG is responsible for reviewing infrastructure-related changes, recommending infrastructure-related transition plans and tech refresh strategies, reviewing infrastructure-related PMRs, and carrying out

actions delegated from the ICCB. The following are designated as AFR representatives and the frequency of this meeting:

4.11.1. Chair: HQ AFRC/A6C.

4.11.2. Secretariat: HQ AFRC/A6C.

4.11.3. Members: HQ AFRC/A6XP Program Managers (PMs), HQ AFRC/A6C Subject Matter Experts (SMEs), Cybersecurity, enclave Information Systems Security Manager (ISSM), other ISSMs.

4.11.4. Meetings: Quarterly at a minimum; additionally at discretion of chair

4.12. **Systems/Application Configuration Control Board (SCCB).** The purpose of the SCCB is to serve as the overarching authority for configuration management of all AFR-developed and/or managed business systems, applications, and capabilities. This includes mobile applications, but not mobile delivery infrastructure capabilities. The SCCB will review and approve configuration changes for enhancements to AFR-unique business systems; approve Courses of Action (COAs) related to potential new software development efforts; review all AFR-unique systems to reduce duplication and look for opportunities for integration with other systems; conduct biannual program management reviews for AFR business systems/ applications/capabilities; approve transition plans for AFR software systems/capabilities; and serve as approval authority for system enhancement actions, to include, but not limited to:

4.12.1. Changes/modifications to an existing capability beyond the sustainment actions AFR functional system configuration control working groups have the authority to approve.

4.12.2. Adding new features, functionality, modules, tools, or service capabilities to an existing system.

4.12.3. Changes to the scope of an existing system.

4.12.4. Creating new applications or systems.

4.12.5. Expansion of existing capabilities to additional AFR user types.

4.12.6. Expansion of existing capabilities to a new external user base.

4.12.7. Expansion, addition or deletion of interfaces for existing system.

4.12.8. Purchases of new hardware or software (to include license renewals and software upgrades) necessary to support system capability changes.

4.12.9. The following are designated as AFR representatives and the frequency of this meeting:

4.12.9.1. Chair(s): Deputy CIO.

4.12.9.2. Secretariat: EA Team.

4.12.9.3. Key Advisors: HQ AFRC/A6T (CTO) & CEA.

4.12.9.4. Members: EA; AFR System PMs/Owners; HQ AFRC/A1; the HQ AFRC/A6 FISMA Accrediting Systems Information Systems Security Managers (ISSM) and Information Systems Security Officers (ISSO); the AFR Portfolio

Manager; Cybersecurity (A6OS); and A6C personnel representing enclave configuration and enterprise operations.

4.12.9.5. Meetings: Monthly

4.13. **Systems/Applications Configuration Control Working Groups (SCCWG).** AFR business system owners must establish individual configuration control working groups to provide oversight of system-specific configuration control issues within their scope and authority. SCCWGs have the authority to approve, prioritize, and manage the following sustainment actions for the system(s) under their purview:

4.13.1. Break/fix actions to correct errors or defects in order to make existing functionality work as designed.

4.13.2. Improvements to user interaction with existing functionality.

4.13.3. System changes to accommodate Laws, Regulations, and Policy (LRP) changes that directly relate to existing functionality.

4.13.4. Modifying or adding workflow, business rules, or reports that support existing capabilities.

4.13.5. Data maintenance (ex: addition and deletion of data tables, fields, and elements).

4.13.6. Commercial-off-the-shelf (COTS) software releases intended to maintain existing operational capability of the system.

4.13.7. Maintain existing technical or performance specifications.

4.13.8. Any changes outside the sustainment scope listed above are considered enhancements and require approval beyond the business system functional configuration control board approval authorities. Requests for enhancement actions must be submitted via the Project, Workflow, Requirements and Resources Manager (PWRR) IT requirements system (**https://pwrr.afrc.af.mil**) for enterprise evaluation and approval. AFR EA/CDO personnel will be assigned to assist PMs with enhancement PWRR submissions. When PMs request that architects submit on their behalf, AFR EA personnel will coordinate PWRR input with system PM prior to submission. PMs are required to support PWRR activities until submission is closed. If immediate review & approval is required, PWRR submission should include rationale for expediting enhancement approval. In the event a Total Force governance structure considers an AFR system as a potential course of action for a Total Force solution, the PM is responsible for coordinating the AFR system input or proposal with the AFR CEA via PWRR prior to providing input or proposal to the Total Force for consideration. Request for coordination on AFR system input for submission to Total Force should be specifically identified in PWRR submission to ensure coordination is expedited. EA POCs are available to assist PM with obtaining AFR CIO coordination.

4.13.9. The following are designated as AFR representatives and the frequency of this meeting:

4.13.9.1. Chair: As determined/chartered by functional directorate; most often is the system PM.

4.13.9.2. Secretariat: As determined/chartered by individual system owners.

4.13.9.3. Members: As determined/chartered by individual Information Systems Owner (ISO), system technical experts, system business function SMEs, system ISSM, and user representatives.

4.13.9.4. Meetings: As determined/chartered by individual system owners.

4.14. **Enterprise Architecture Board (EAB).** The purpose of the EAB is to oversee and manage AFR architectural efforts, to include establishing strategic vision, setting priorities, developing architectural artifacts, determining potential COAs for requests related to potential new software development efforts, recommending COA decisions to the SCCB, determining Business Process Reengineering (BPR) efforts to be undertaken by EA, and managing EA program maturity efforts. The following are designated as AFR representatives and the frequency of this meeting:

4.14.1. Chair: Deputy CIO.

4.14.2. Secretariat: EA Team.

4.14.3. Members: CEA, CTO, EA team, Cybersecurity (A6OS), Functional Directorate POCs and customer representation.

4.14.4. Meetings: 2x monthly.

4.15. **Enterprise Architecture Working Group (EAWG).** The purpose of the EAWG is to provide a standing forum for EA team discussion of current architecture topics, architecture repository environment, team assignments, and progress carrying out EA Board direction. The EAWG also identifies issues to be elevated to EA Board. The following are designated as AFR representatives and the frequency of this meeting:

4.15.1. Chair: CEA.

4.15.2. Secretariat: EA team.

4.15.3. Members: EA team.

4.15.4. Meetings: Weekly.

4.16. **AFR Data Board.** The purpose of the AFR Data Board is to organize formal data activities and processes across the AFR Component based on data and information subject areas. The AFR Data Board advises and oversees implementation of all data issues to include data governance; strategic use of data to meet mission needs; internal and external use and sharing of AFR data; data compliance, registration, and protection; data quality; internal and external data policies and procedures; data architectures; meta-data repositories, and data management performance measures. The AFR Data Board oversees data stewardship for AFR authoritative data sources (ADS) and coordinates new or decommissioned ADSs with the Office of the AF Chief Data Officer. The following are designated as AFR representatives and the frequency of this meeting:

4.16.1. Chair: Deputy CIO.

4.16.2. Secretariat: EA team.

4.16.3. Members: CDO, Cross-functional group of coordinating Dataset Leads responsible for support and oversight of a particular data management initiative launched by the DMB, plus functional and technical SMEs throughout the organization.

4.16.4. Meetings: twice per month.

4.17. **AFR Data Working Group (DWG).** The purpose of the AFR DWG is to organize formal data activities and processes across the AFR Component based on data and information subject areas. The AFR DWG advises and oversees implementation of all data issues to include data governance; strategic use of data to meet mission needs; internal and external use and sharing of AFR data; data compliance, registration, and protection; data quality; internal and external data policies and procedures; data architectures; meta-data repositories, data management performance measures, Service Oriented Computing Environment (SOCE) and Decisional Data Store (DDS). The AFR DWG oversees data stewardship for AFR authoritative data sources (ADS), coordinates new or decommissioned ADSs with the Office of the AF Chief Data Officer, oversees service oriented capabilities and processes on Non-classified Internet Protocol Router Network (NIPR) and Secret Internet Protocol Router Network (SIPR) and covers all DDS/Shared Data Environment issues. The following are designated as AFR representatives and the frequency of this meeting:

4.17.1. Chair: CDO.

4.17.2. Secretariat: EA team.

4.17.3. Members: Cross-functional group of coordinating Dataset Leads responsible for support and oversight of a particular data management initiative launched by the DMB, plus functional and technical SMEs throughout the organization.

4.17.4. Meetings: 2x a month.

4.18. **Cybersecurity.** The AFRC Cybersecurity function aligns with the National Institute for Standards and Technology (NIST) Committee of National Security Systems Policy (CNSSP), Office of Management and Budget (OMB), Federal Information Processing Standard (FIPS), Department of Defense Instruction (DoDI), AF, AFRC and Risk Management Framework (RMF) Cyber Security Implementation Standards representing a dynamic, multi-disciplinary set of challenges. Specific responsibilities include:

4.18.1. Oversees key CIO processes related to Assessment & Authorization (A&A), FISMA, RMF and Command Cyber Readiness Inspection (CCRI).

4.18.2. Serve as a member of the ICCB, EAB and SCCB.

4.18.3. Proposes CIO policy and guidance related to areas of key CIO responsibilities.

4.18.4. Maintains process guidance for key CIO processes in area of responsibility.

4.19. **Cyber Workforce Management.** AFR Cyber Workforce Management functions:

4.19.1. Oversees key CIO processes related to DTs, Career Field Management, and 8140 tracking.

4.19.2. Ensure cybersecurity workforce is identified, trained, certified, qualified, tracked, and managed.

4.19.3. Report the status of their cybersecurity workforce (civilian, military, and contractors).

4.20. **IT Funding and IT Tech Strategy.** IT Funding and IT Tech Strategy functions:

4.20.1. Oversees key CIO processes related to funds management, requirements processing, Unfunded Requirements (UFR) process, portfolio management, and IT contract reviews.

4.20.2. OPR for IT funding and co-OPR for IT tech strategy.

4.20.3. Oversees key CIO processes for A6X infrastructure PMRs and IT Blueprints.

4.20.4. Maintains process guidance for key CIO processes in area of responsibility.

4.20.5. Proposes CIO policy and guidance related to areas of key CIO responsibilities.

4.20.6. Serves as AFR CIO Portfolio manager, overseeing development of IT portfolio for presentation to AFR CIO.

4.20.7. Maintains AFR CIO IT expenditure decision support tools.

4.20.8. Works with A4 to ensure AFR Facilities Sustainment, Renovation, and Modernization (FSRM).

4.20.9. Integrated Priority List (IPL) and CIO IT unfunded list are cross-referenced and associated IT needs are accounted for as needed and appropriately prioritized on the CIO IT funded list.

4.20.10. Schedules Program Management Reviews for all IT programs.

4.20.11. Chairs AFR IT Funding Board.

4.20.12. Provides secretariat support for CIO Advisory Committee, IT Program Review Panel, and IT Funding Board.

4.20.13. Serves as liaison with AFR's assigned 38th ES Cyber Systems Integrator-Command (CSI-C) for issues supported by the CSI community.

4.20.14. Serves as subject matter expert/advisor regarding AFR CIO governance structure.

4.20.15. Maintains overarching AFR CIO governance structure charter.

4.20.16. Oversees IT Unfunded requirements.

4.20.17. Maintains AFR CIO site on Internal Control Measure (ICM) Key Forums.

4.20.18. Serves as secretariat for CIO Advisory Committee and IT Funding Board.

5. CIO Implementation Guidance. This AFRCI is only intended to define the overall scope, structure, roles, and responsibilities associated with implementing CIO responsibilities within AFR. The **s**pecific goals, policies, processes, procedures, guidance, performance measures and other details required to implement the full range of CIO responsibilities defined in this AFRCI will be issued, distributed and maintained by AFR CIO, CTO, CEA/CDO, CIO-related Board/Group chairs, A6 division chiefs, and/or other appropriate OPRs separately from this document and may be accessed via the AFR CIO area on Key Forums within the HQ AFRC SharePoint ICM.

JERALD H. NARUM, Col, USAF
Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 17-140, *Architecting*, 29 June, 2018

AFI 33-360, *Publications and Forms Management*, 1 December 2015

AFMAN 17-402, *Clinger Cohen Act (CCA) Compliance*, 20 June 2018

AFMAN 63-144, *Business Capability Requirements, Compliance, and System Acquisition*, 25 July 2018

AFPD 17-1, *Information Dominance Governance and Management*, 12 April 2016

AFPD 17-2, *Cyberspace Operations*, 12 April 2016

CJCSI 3170.01H, *Joint Capabilities Integration and Development System (JCIDS)*, 10 January 2012

CJCSI 6212.01F, *Net Ready Key Performance Parameters*, 21 March 2012

DoD CIO Memorandum, "DoD Net-Centric Data Strategy," 2 May 2003

DoD CIO Memorandum, "DoD Net-Centric Services Strategy," 4 May, 2007

DoD Data Services Environment (DSE) Concept of Operations (CONOPS), 2 Aug 2013

DoDI 5000.75, *Business System Requirements and Acquisition*, 2 February 2017

DoDI 8320.ff, *Implementing the Sharing of Data, Information, and IT Services in the DoD*, 18 August 2011

H.R.4174 Foundations for Evidence-Based Policymaking Act

National Defense Authorization Act (NDAA) for Fiscal Year 2012

USAF Data Framework, 23 May 2017

USAF Data Services Reference Architecture, 2 Feb 2019

Prescribed Forms

No Forms Prescribed

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

A&A—Assessment and Authorization

ACS—Agile Combat Support

ADS—Authoritative Data Sources

AFB—Air Force Base

AFDP—Air Force Data Panel

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFR—Air Force Reserve

AFRC—Air Force Reserve Command

AFRIMS—Air Force Records Information Management System

ANG—Air National Guard

ARPC—Air Reserve Personnel Center

BPR—Business Process Reengineering

CC—Commander

CCRI—Command Cyber Readiness Inspection

CDO—Chief Data Officer

CEA—Chief, Enterprise Architecture

CFM—Career Field Manager

CIO—Chief Information Officer

CNSSP—Committee of National Security Systems Policy

COA—Course of Action

CONOPS—Concept of Operations

COTS—Commercial-Off-the-Shelf

CSI—Cyber Systems Integrator-Command

CTO—Chief Technical Officer

DDS—Decisional Data Store

DT—Developmental Team Board

DWG—Data Working Group

EA—Enterprise Architecture

EAB—Enterprise Architecture Board

EAWG—Enterprise Architecture Working Group

ECCB—Enterprise Configuration Control Board

EIS—Enterprise Information Services

FIPS—Federal Information Processing Standard

FISMA—Federal Information Security Management Act

HAF—Headquarters Air Force

H.R—Human Resources

HQ—Headquarters

IAO—Information Assurance Officer

ICCB—Infrastructure Configuration Control Board

ICCWG—Infrastructure Configuration Control Working Group

ICM—Internal Control Measure

ISO—Information Security Officer

ISSO—Information System Security Officer

IPL—Integrated Priority List

ISO—Information Security Officer

ISSM—Information Systems Security Manager

ISSO—Information Systems Security Officer

IT—Information Technology

ITMRA—Information Technology Management Reform Act

LRP—Laws Regulations, and Policy

NAF—Numbered Air Force

NIST—National Institute for Standards and Technology

NIPR—Non-classified Internet Protocol Router Network

NSS—National Security System

OMB—Office of Management and Budget

OPR—Office of Primary Responsibility

PFM—Program Financial Management

PM—Program Manager

PMR—Program Management Review

POM—Program Objective Memorandum

PWRR—Project, Workflow, Requirements and Resources Manager

RDS—Records Disposition Schedule

RMF—Risk Management Framework

SAF—Secretary of the Air Force

SCCB—System/Application Configuration Control Board

SCCWG—Systems/Applications Configuration Control Working Group

SDDP—Service Development and Delivery Process

SIPR—Secret Internet Protocol Router Network

SME—Subject Matter Expert

SOCE—Service Oriented Computing Environment

USAF—United States Air Force

Attachment 2

AFR ENTERPRISE ARCHITECTURE PROGRAM

A2.1. AFR Enterprise Architecture Program. This charter outlines the purpose, authority, background, and scope of Air Force Reserve (AFR) Enterprise Architecture (EA) program.

A2.2. PURPOSE. The purpose of the EA program is to provide authoritative reusable architecture and analysis to support different decision processes, support investment compliance, comply with acquisition requirements, support the requirements processes, and to enable the determination and justification of courses of actions in order to provide guidance for Information Technology (IT) capital investment decisions.

A2.3. AUTHORITY. This charter operates under the authority of Chief of Air Force Reserve and will serve as a guide for AF/RE, Headquarters Air Force Reserve Command (HQ AFRC), and AFRC Numbered Air Forces (NAFs) and units, Force Generation Center (FGC), and Air Reserve Personnel Center (ARPC) to understand the AFR EA program. The mandates to implement an EA program are as follows:

A2.3.1. CJCSI 3170.01H, *Joint Capabilities Integration and Development System (JCIDS)*

A2.3.2. Tailored Information Support Plan (TISP) - DoD CIO Memorandum, Interim Guidance for the Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)

A2.3.3. CJCSI 6212.01F, *Net Ready Key Performance Parameters*

A2.3.4. AFMAN 17-402, *Clinger Cohen Act (CCA) Compliance*

A2.3.5. National Defense Authorization Act (NDAA) for Fiscal Year 2012

A2.3.6. AFPD 17-1, *Information Dominance Governance and Management*

A2.3.7. AFI 17-140, *Architecting*

A2.3.8. DoDI 5000.75, *Business System Requirements and Acquisition*

A2.3.9. AFMAN 63-144, *Defense Business System Life Cycle Management*

A2.4. EA BACKGROUND.

A2.4.1. According to AF Architecting Concept of Operations (Dec 2009), architecture should enable the delivery of timely, relevant, unambiguous information to support informed decision-making by Air Force leaders to maximize military capabilities while optimizing allocation of resources. The Air Force and DoD use EA to support key processes for requirements, acquisition, systems engineering, programming and budgeting of funds, interoperability, and portfolio management (AFI 17-140).

A2.4.2. AFR uses architecture to unravel the complexity of our business systems, processes, data, and programs. EA is not just about IT. EA helps reveal interdependent relationships to decision-makers in an easily understandable format to inform decision-making and ensure alignment of business and technology to strategies. The architecture can be used to identify and eliminate duplicative investments, identify services and applications reuse opportunities, build efficiencies, increase automation, improve mission performance through reengineered processes, enhance information sharing through data and system integration, and optimize

resource utilization. The AFR EA program requires continuous teamwork and partnership across business domain stakeholders, data stewards, and IT system program managers. When creating EA products, the AFR EA program will: utilize the latest version of Department of Defense Architecting Framework (DoDAF); consider the current ("as-is") and target ("to-be") architecture; and collaborate with stakeholders to develop transition plans for migrating from the current to the target architecture. Specific guidance for developing AFR products can be found in the AFR EA modeling standards governance document. The AFR EA program helps drive process-derived solutions across the entire Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Process (DOTMLPF-P) spectrum.

A2.5. OBJECTIVES.

A2.5.1. Enterprise Architecture is an organizational strategic asset that represents an investment in the organization's future. It is a corporate investment to produce strategic mission value (results and outcomes). To accomplish this, the EA program will focus on these objectives:

A2.5.1.1. Cost Reduction and Technology Standardization. This includes savings through elimination of duplicative investments, reusing applications, retirement of aging and high-cost systems and platforms, and improved mission performance and efficiencies through modernized supporting systems.

A2.5.1.2. Identify Efficiencies. Use architecture to identify redundancies, technology gaps, automation opportunities, and business process improvement.

A2.5.1.3. Support Technology Acquisitions. Build architecture to clearly define new requirements, meet governance compliance, and ensure solutions intended to achieve the mission align to AFR strategy.

A2.5.1.4. Provide Analysis. Use architecture to perform analysis in support of leadership decisions and course of action (COA) selections.

A2.5.1.5. Mature the EA Program. Continue to evaluate the Program's practices, structures, and activities to progress to increasingly higher states of maturity thereby maximizing its chances of realizing EA's institutional value.

Attachment 3

AFR DATA PROGRAM

A3.1. AFR Data Program. This charter outlines the purpose, background, and objectives in the AFR Data program. The Chief Data Office is established to drive the Air Force Reserve's evolution to an environment in which data is shared and leveraged as a strategic asset.

A3.2. PURPOSE. The Chief Data Office will set the AFR strategy, policies, standards and governance to ensure data is secure, visible, accessible, understandable, linked, and trustworthy for the Air Force Reserve and mission partners. This charter's purpose is to establish a base level of support that meets and exceeds the data and information needs of all AFR business operations and enterprise stakeholders in terms of data availability, security, and quality.

A3.3. AUTHORITY. This charter operates under the authority of Chief of Air Force Reserve and will serve as a guide for AF/RE, Headquarters Air Force Reserve Command (HQ AFRC), and AFRC Numbered Air Forces (NAFs) and units, Force Generation Center (FGC), and Air Reserve Personnel Center (ARPC) to understand the AFR Data Program. The mandates to implement Data Management are as follows:

A3.3.1. H.R.4174 Foundations for Evidence-Based Policymaking Act

A3.3.2. DoD CIO Memorandum, "DoD Net-Centric Data Strategy"

A3.3.3. DoD CIO Memorandum, "DoD Net-Centric Services Strategy"

A3.3.4. DoDI 8320.ff, *Implementing the Sharing of Data, Information, and IT Services in the DoD*

A3.3.5. DoD Data Services Environment (DSE) Concept of Operations (CONOPS)

A3.3.6. USAF Data Services Reference Architecture

A3.3.7. USAF Data Framework

A3.4. BACKGROUND. The AFR Chief Data Officer (CDO) was designated by the Chief of Air Force Reserve to improve mission effectiveness and efficiency. The Chief Data Office, now residing in A6, exists to:

A3.4.1. Facilitate data management and analytics collaboration.

A3.4.2. Leverage data and information as enterprise assets.

A3.4.3. Enable more agile solutions and services made possible through shared data.

A3.5. OBJECTIVES.

A3.5.1. The Chief Data Office's primary responsibility is to strategically manage and exploit the information assets of the Air Force, especially Air Force Reserve, toward optimizing readiness, driving innovation and improving AFR mission effectiveness and efficiency. To accomplish this responsibility, the Chief Data Office will focus on these program objectives:

A3.5.1.1. Develop Data Strategy. Develop and implement an enterprise-level Air Force Reserve Data Strategy for leveraging data as a strategic asset.

A3.5.1.2. Identify Enterprise Data Capabilities. Define and recommend the enterprise-wide capabilities needed to achieve the AF Data Strategy.

A3.5.1.3. Establish Use. Develop and implement requisite Concept of Operations (CONOPS) for employing the capabilities needed to achieve the AF Data Strategy.

A3.5.1.4. Share Data. Define an architectural framework and establish a technology platform to enable enterprise analytics and deliver enterprise data services to enable more agile solutions made possible by data sharing and reuse.