DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES AIR FORCE
WASHINGTON, DC

DAFGM2023-32-02
17 AUGUST 2023

MEMORANDUM FOR DISTRIBUTION C
MAJCOMs/FOAs/DRUs/ FLDCOMs

FROM: HQ USAF/A4C
1260 Air Force Pentagon Washington
DC 20330-1260

SUBJECT: Department of the Air Force Guidance Memorandum, Establishing *Civil Engineer Enterprise Governance for Information Technology*

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

RELEASIBILITY: There are no releasability restrictions on this publication.

OPR: AF/A4CS, Systems & Data Division

By Order of the Secretary of the Air Force, this Guidance Memorandum establishes enterprise governance for Civil Engineer (CE) Information Technology (IT). Compliance with this memorandum is mandatory. To the extent its directions are inconsistent with other Department of the Air Force (DAF) publications, the information herein prevails in accordance with Department of Air Force Instruction (DAFI) 90-160, *Publications and Forms Management.*

This guidance is applicable to the entire DAF, including the United States Air Force (USAF), the United States Space Force (USSF), the Air Force Reserve, the Air National Guard, the Civil Air Patrol, when conducting missions as the official Air Force Auxiliary, all DAF civilian employees, and those with a contractual obligation to abide by the terms of DAF issuances and who develop, acquire, deliver, use, operate, manage, or maintain CE IT. This Department of Air Force Guidance Memorandum (DAFGM) does not address Control Systems Cybersecurity. For guidance on this topic, refer to DAFGM 2022-32-01, *Civil Engineer Control Systems Cybersecurity*.

Refer recommended changes and questions about this publication to the Office of Primary Responsibility using DAF Form 847, *Recommendation for Change of Publication*, routed through chain of command. 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 DAFMAN 90-161, Publishing Processes and Procedures, 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 requestor's commander for non-tiered compliance items. Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction 33-322, Records Management and Information Governance Program, and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System.

This Memorandum becomes void after one year has elapsed from the date of this Memorandum, or upon publishing of a new publication permanently establishing this guidance, whichever is earlier.

TOM D. MILLER
Lieutenant General, USAF
DCS/Logistics/ Engineering & Force Protection

Chapter 1
PURPOSE, OBJECTIVES, AND SCOPE

1.1. Purpose. The purpose of this DAFGM, *Civil Engineer (CE) Enterprise Governance for Information Technology (CEEG-IT)*, is to provide a framework governing the DAF CE Enterprise in the areas of IT strategy development, portfolio direction setting, decision making process formalization, and enterprise-wide initiative identification. This DAFGM formalizes roles and responsibilities for managing and operating CE IT and outlines the DAF CE IT Governance structure and processes.

1.2. Objectives. The objectives of this DAFGM are to:

1.2.1. Ensure every CE enterprise decision maker involved in assessment, planning, programming and/or execution has the necessary infrastructure, equipment, tools, and relevant and timely information to support their respective missions.

1.2.2. Ensure all CE enterprise stakeholder IT interests and missions are properly represented and prioritized in accordance with their respective roles, responsibilities, and authorities.

1.2.3. Ensure all CE enterprise IT decisions and actions are in proper alignment with higher authority, policy, and guidance as part of the Planning, Programming, Budgeting and Execution (PPBE) process. This will be accomplished through alignment to the Business Capability Acquisition Cycle (BCAC) per Department of Defense Instruction (DoDI) 5000.75_DAFI63-144, Business Systems Requirements and Acquisition.

1.2.4. Provide an overarching framework for governing CE IT processes at the DAF level and strategically align them with the processes of the DAF CE IT Enterprise across all organizations and program areas. Provide guidance regarding CE IT related policy, oversight, resourcing, and execution in support of the DAF CE Enterprise and identified strategic priorities.

1.2.5. Champion the need for stakeholders across the DAF CE Enterprise to liaison with the Air Force Installation and Mission Support Center (AFIMSC) Corporate Structure, the Air Force Corporate Structure (AFCS), and other DAF governing bodies as necessary to ensure CE IT requirements are appropriately resourced.

1.3. Scope. This DAFGM and the CEEG-IT governance framework applies to all CE Enterprise IT systems, IT platform requirements, and data-enabling capabilities to deliver Air Force Civil Engineer Center (AFCEC) core capabilities through a Unity of Effort (UoE) per the October 2022 AFCEC Management Plan, version 3.0. CE Enterprise IT is defined as IT in the Business Mission Area (BMA) Real Property sub-portfolio, or IT funded within Program Element Codes (PECs) commonly aligned with CE (e.g., Facility Operations, Facilities Sustainment Restoration and Modernization, etc.), or IT required as a material solution to 32-Series DAF Policy Documents and/or DAFIs. CEEG-IT governs new CE IT capability requests (ITCRs), requests for enhancement to existing CE IT enterprise systems, IT system sustainment requirements, and all other enterprise-level CE IT related investment decisions.

1.3.1. Innovation and/or pilot efforts specific to CE that include IT requirements differ from CE IT sustainment and/or new IT capability requests and do not formally process through CEEG-IT. Instead, this DAFGM outlines how AFCEC will guide proponents through Assessment & Authorization (A&A) necessary to obtain Authority to Operate (ATO) and/or Interim Authority to Test (IATT) for CE IT innovation and/or pilot efforts in **Chapter 4.**

1.3.2. IT Systems are defined by the National Institute of Standards and Technology (NIST) as: any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

1.3.3. IT Platforms are defined by NIST as: a computer or hardware device and/or associated operating system, or a virtual environment, on which software can be installed or run.

1.3.4. IT Asset Management (e.g., IT licenses, IT software, IT hardware) and Operational Technology (OT) fall outside the purview of this DAFGM. For additional guidance specific to these topics, refer to DAFMAN 17-1203, *Information Technology Asset Management (ITAM),* and DAFGM 2022-32-01, *Civil Engineer Control Systems Cybersecurity*.

1.3.5 IT compliance for previously capitalized investments now falls within the purview of this DAFGM. For additional guidance specific to this topic, refer to AFI 17-110, Information Technology Portfolio Management and Capital Planning and Investment Control.

1.3.6. The CEEG-IT framework is detailed in **Chapter 3** and spans several DAF organizations that support the development of new capabilities, and includes operational level bodies that support the capture, analysis, and development of functional requirements. CE IT Enterprise stakeholders and detailed roles and responsibilities for each are outlined in **Chapter 2.**

Chapter 2
STAKEHOLDERS, ROLES, AND RESPONSIBILITIES

2.1. Introduction. The following organizations comprise the team members supporting CE IT across the DAF CE Enterprise for Business Mission Area (BMA) systems. BMA, Warfighting Mission Area, and Defense Intelligent Mission Area systems are defined in Attachment A**.** All stakeholders are subject to the roles and responsibilities outlined in the applicable IT regulations detailed in **Table 8.1.** of AFI 63-101_20-101, *Integrated Life Cycle Management*, in addition to the roles detailed below.

2.2. DAF Stakeholders.

2.2.1. DAF Chief Information Officer (SAF/CN). SAF/CN provides policy and strategic direction for Enterprise Information Technology (EIT), governance, standards, interoperability, and cyber security, including oversight and management of the Non-Secure Internet Protocol Router (NIPR) Network and Secure Internet Protocol Router (SIPR) Network infrastructure for the DAF.

2.2.1.1 SAF/CN attends the A4 Portfolio Board (A4 PB) as an advisory member, to support final Milestone Decision Authority (MDA) approval on prospective CE IT Requests and/or BCAC Authority to Proceed (ATP) decision points.

2.2.1.2 BCAC is a process utilized by DoD programs to streamline the acquisition, development, deployment, and maintenance of business systems, aligning with commercial best practices, and minimizing the need for customization where possible. For more guidance on the BCAC process, review DODI 5000.75_DAFI63-144.

2.2.2. Deputy Chief Management Officer and Office of Business Transformation (SAF/MG). SAF/MG will:

2.2.2.1. Perform functions as detailed in AFI 17-110, *Information Technology Portfolio Management and Capital Planning and Investment Control* to include defense business system accountability and modernization.

2.2.2.2. Attend the A4 PB as a Tri-Chair, provide final approval on prospective CE IT Requests and/or BCAC ATP decision points where the CMO is the designated ATP decision authority.

2.2.3. The Assistant Secretary of the Air Force for Acquisition, Technology and Logistics (SAF/AQ). SAF/AQ will:

2.2.3.1. Ensure all CE IT related acquisition and sustainment programs comply with requirements in AFI 17-110.

2.2.3.2. Provide an advisor to the A4 PB, to facilitate final approval on prospective CE IT Requests and/or BCAC ATP decision points.

2.2.4. The Assistant Secretary of the Air Force for Installations, Environment and Energy (SAF/IE). SAF/IE will:

2.2.4.1. Provide policy, strategic direction, priorities, doctrine, directive guidance, and oversight on the management and execution of programs within this area of responsibility per HAFMD 1-18, *Assistant Secretary of The Air Force (Installations, Environment and Energy)*.

2.2.4.2. Engage with the Office of the Secretary of Defense, Joint Staff, other Services, DAF, Congress, international partners, and other federal and non-federal agencies in matters supporting programs within this area of responsibility.

2.2.4.3. Advocate for resources within the DAF Corporate Structure in support of the development and oversight of an integrated strategy for CE IT.

2.2.4.4 Identify gaps in resources when standards change and bring them into the corporate process**.**

2.2.5. The Deputy Assistant Secretary of the Air Force (Environment, Safety, and Infrastructure) (SAF/IEE). SAF/IEE is delegated authority for matters related to this instruction and will:

2.2.5.1. Send appropriate representatives to advise on A4 PB matters at their discretion. **(T-1)**

2.2.5.2. When requirements dictate, provide a representative, policy expert and/or administrative support to advise the AFCEC chaired Requirements, Engagements and Acquisitions Panel (REAP) to address questions, provide guidance for AFCEC REAP operations, and determine topics to be presented to the appropriate body. **(T-1)**

2.2.6. Deputy Assistant Secretary of the Air Force (Installations) (SAF/IEI). SAF/IEI is delegated authority for matters related to this instruction and will:

2.2.6.1. Send designated representatives to weigh in on A4 PB matters at their discretion. **(T-1)**

2.2.6.2. When requirements dictate, provide a representative, policy expert and/or administrative support to the AFCEC REAP to address questions, provide guidance for AFCEC REAP operations, and determine topics to be presented to the appropriate body. **(T-1)**

2.3. A4 Stakeholders.

2.3.1. The Deputy Chief of Staff, Logistics, Engineering and Force Protection (AF/A4). Based on AF/A4 responsibilities in HAFMD 1-38, *Deputy Chief of Staff, Logistics, Engineering and Force Protection* ensures AF/A4 acts as AF/A4 Chief Information Officer (CIO) and Chief Architect for Logistics, Engineering, and Force Protection (LEFP) IT Portfolios. **(T-1)**

2.3.1.1. AF/A4 appoints the AF/A4 Data Officer and AF/A4 Artificial Intelligence Liaison. **(T-1)**

2.3.1.2. Provide overall Basing and Logistics Enterprise Strategy (BLES).

2.3.1.3. Coordinate with AF/A4C and AFIMSC on LEFP matters that affect CE IT and Data policy.

2.3.2. Director of Resource Integration (AF/A4P). The Director of Resource Integration (AF/A4P) reports to the AF/A4 and is responsible for integration of the Air Force BLES. AF/A4P will:

2.3.2.1. Serve as the AF/A4 appointed CIO for the LEFP IT Portfolios, based on responsibilities in HAFMD 1-38. As the AF/A4 CIO, AF/A4P may delegate responsibilities and authority of the A4 Data Officer (DO) and Chief Architect (CA) for LEFP IT portfolio. **(T-1)**

2.3.2.2. Serve as the Logistics Authorizing Official (AO) for IT systems on the Logistics Authorized Boundary List (ABL) in accordance with HAFMD 1-38 and ensures IT system compliance with AFI 17-101, *Risk Management Framework (RMF) For Air Force Information Technology (IT),* and DAF RMF Knowledge Service (KS). **(T-1)**

2.3.2.3. Develop and guide implementation of LEFP IT Strategy, plans, policy, governance, Business Enterprise Architectures (BEA), standards, resources, and investments. **(T-1)**

2.3.2.4. Develop and exercise oversight responsibilities of LEFP IT Portfolio Organizational Execution Plan to include aligning IT Investments to Strategic Management Plan and Functional Strategies. **(T-1)**

2.3.2.5. Provide oversight across both Joint and Air Force Global Combat Support Families of Systems, containing diverse logistics management information systems requirements. **(T-1)**

2.3.2.6. Be responsible for the planning, management, and reporting of process improvement and business transformation across the Logistics, Civil Engineer, and Security Forces communities through employment of continuous process improvement methodologies and application of BCAC. **(T-1)**

2.3.2.7. Represent A4 at the Business Mission Area Council for BMA governance hosted by SAF/MG. **(T-1)**

2.3.2.8. Serve as a tri-chair for decision making on BCAC matters in the A4 PB. **(T-1)**

2.3.2.9. Advocate for IT resource support for Logistics, Security Forces and Civil Engineers through the DAF Corporate Structure, informed by inputs from MAJCOMs, AFIMSC, and A4 Directorates. **(T-1)**

2.3.3. Logistics Chief Information Officer Support Division (AF/A4PA). AF/A4PA will:

2.3.3.1. Serve as the A4 DO/CA (under the authority of the A4 CIO), oversee the A4 Enterprise Architecture, and guide the implementation of LEFP data and technology integration strategy, plans, policy, governance, BEAs, standards, resources, and investments. **(T-1).** A4 Data Officer, CE Domain Data Representative, AFIMSC Principal Data Steward, Operational Level Domain Data Steward, Data Integration Officer, and Functional Data Steward roles and responsibilities are outlined within the *AF/A4 Data Stewardship Framework*. A4 Enterprise Architect, CE Segment Chief Architect, Operational Level Segment Architect, and Tactical Level Solution Architect roles and responsibilities are outlined within the *AF/A4 EA Framework* and AFI 17-140, *Architecting* documents.

2.3.3.2. Serve as the cross functional champion for A4 Data, Architecture, Analytics, and Artificial Intelligence (DA3) capabilities that support and align to DAF and DoD goals in accordance with HAFMD 1-38. **(T-1).** Ensure all A4 Data is Visible, Accessible, Understandable, Linked, Trusted, Interoperable and Secure (VAULTIS). **(T-1)**

2.3.3.3. Serve as the Secretariat for the A4 PB. These duties include, but are not limited to, scheduling and facilitating meetings, building agendas, organizing, and disseminating briefing materials, developing business rules, and other administrative requirements requested by the supported body. **(T-1)**

2.3.3.4. Participate as a core member of the AFCEC Roundtable and advisory member of the AFCEC REAP (as requirements dictate) to assist with request assessments and provide relevant visibility as the Secretariat of the AF Portfolio Board. **(T-1)**

2.3.3.5. Lead and chair the A4 Data, Architecture and Analytics Working Group (DAAWG) to ensure enterprise data consistency and oversee the data strategy, policy, and governance for A4 data. Approve architecture content captured within the A4 enterprise architecture as well as reference architecture content and updates impacting enterprise-level alignment. Capture and maintain strategic alignment of CE segment-level and solution-level architectures to the A4 EA. **(T-1)**

2.3.3.6. Serve as the representative to the DAF Data and Artificial Intelligence (AI) Board and provide recommendation for representatives to DAF Data and AI Working Groups. **(T-1)**

2.3.3.7. Serve as a core member of the AFCEC Roundtable **(T-1)**

2.3.3.8. Assist with assessment of CE IT requests and provide support with the BCAC process when CE IT acquisitions are under consideration. **(T-1)**

2.3.4. The Director of Civil Engineers (AF/A4C). The Director of Civil Engineers (AF/A4C) will:

2.3.4.1. Provide program functional oversight for matters related to CE IT. The A4C will coordinate IT related strategy with A4PA and AFIMSC to ensure consistency and alignment between organizations. **(T-1)**

2.3.4.2. Advocate for resources to support CE IT through AFIMSC and the DAF Corporate Structure in accordance with A4 data and CIO standards. **(T-1)**

2.3.4.3. Provide a representative to A4 Portfolio Board and Data Working Groups. **(T-1)**

2.3.5. The Deputy Director of Civil Engineers (AF/A4C-2). AF/A4C-2 will serve as the CE IT Systems and IT Platforms AO, with responsibilities described in AFI 17-101. **(T-1)**

2.3.6. The A4C Systems Division (AF/A4CS). AF/A4CS will:

2.3.6.1. Be responsible for oversight, policy, planning and funding advocacy for CE IT systems across the AF Enterprise. **(T-1)**

2.3.6.2. Develop strategic guidance and coordinate policy in support of CE IT portfolio management

to ensure CE capabilities, processes, procedures, roles, and responsibilities are all codified and executed effectively and efficiently. **(T-1)**

2.3.6.3. Serve as the Authorizing Officials Designated Representative (AODR) for CE IT systems on the CE ABL for the CE IT Systems and IT Platforms AO (A4C2) in accordance with HAFMD 1-38 and ensures IT system compliance with AFI 17-101. **(T-1)**

2.3.6.4. The AODR will coordinate adjustments to the CE ABL with A4PA to ensure the AODR and Security Control Assessor are adequately resourced. **(T-1)**

2.3.6.5. Serve as the CE Domain Data Representative and CE Segment Chief Architect to oversee strategic guidance, direction, policy, and governance to ensure CE data is VAULTIS in accordance with the *DAF Implementation Plan* to the *DoD Data Strategy*. **(T-1)**

2.3.6.6. The CE Segment Chief Architect manages the segment-level and solution-level architectures under their purview and ensures strategic alignment to architecture above them. **(T-1)**

2.3.6.7. Monitor individual CE IT Program Management Office (PMO) efforts to ensure system security certification through Security Control Assessor staff and facilitates an organizational culture with a strong security posture. **(T-1)**

2.3.6.8. Perform administrative duties including, but not limited to, scheduling and facilitating meetings, building agendas, organizing, and disseminating briefing materials, developing business rules, and other administrative requirements requested by the supported body. **(T-1)**

2.3.6.9. Serve as a core member of the AFCEC Roundtable and advisory member of the AFCEC REAP. **(T-1)**

2.3.6.10. Assist with assessment of CE IT requests and provide support with the BCAC process when CE IT acquisitions are under consideration. **(T-1)**

2.3.7. AF/A4C Functional Division Chiefs. Functional Division chiefs, in their capacity as chairs or administrators providing functional validation, will be part of the review and approval of requests elevated from AFIMSC, AFCEC, ANG, AFRC, or other groups, prior to a request entering the formal CEEG-IT process. (T-1)

2.3.8. Air Force Reserve Command (AFRC) and National Guard Bureau (NGB). Representatives from AFRC and the NGB will:

2.3.8.1. Ensure AFRC and NGB compliance with processes outlined in DODI 5000.75_DAFI63-144 for any AFRC or NGB generated IT requirements. **(T-1)**

2.3.8.2. Bring CE IT requirements forward for review and approval through the Intake and Governance processes detailed in **Chapter 4** and champion AFRC and/or NGB generated IT requirements through the BCAC process. **(T-1)**

2.3.9. MAJCOM/A4's, Commanders of Direct Reporting Units (DRUs), Field Commands, National Guard Bureau (NGB/A4), Air Force Reserve Command (AFRC/A4), will:

2.3.9.1. Bring new CE IT requirements forward for review and approval through the CEEG-IT using processes established within this DAFGM. Since CE funds are invested to satisfy CE requirements, non-CE IT requirements will need to be addressed/funded by appropriate domain IT functionals. **(T-1)**

2.3.9.2. These may include IT requirements generated by non-CE functionals that can be delivered using CE IT systems or platforms. **(T-1)**

2.3.9.3. Bring information forward about MAJCOM, NGB and/or AFRC funded CE IT investments, in coordination with the AFCEC Functional Management Office (AFCEC/FMO), support efforts to consolidate systems in accordance with CE IT strategic initiatives and ensure system compliance with AFI 17-110. **(T-1)**

2.3.9.4. AFIMSC/AFCEC shall manage hardware/software funding and accreditation of systems on

behalf of the support theater and combatant command (COCOM) functions with assistance from AFIMSC. **(T-1)**

2.3.9.5. MAJCOMs (or USSF equivalent) will ensure systems supporting theater and COCOM functions are resilient and flexible to adapt to changing contested environments within the AOR. **(T-1)**

2.4. AFMC Stakeholders.

2.4.1. Commander, Air Force Materiel Command (AFMC/CC). AFMC will advocate for resources to support CE IT on behalf of AFIMSC and AFCEC through the DAF Corporate Structure. **(T-1).** AFMC will also have overall responsibility for and support oversight of AFIMSC's roles for resource advocacy and CE IT Strategy development. **(T-1)**

2.4.2. AFMC's Assurance Division (A6I). A6I has overall responsibility for, and supports oversight of, CE IT Business Enterprise System Portfolio Management as executed by AFCEC/FMO and will consult on CE IT-related strategy. Supports CE IT Portfolio IAW 17-110, Roles & Responsibilities, Portfolio Managers. **(T-1)**

2.4.3. Air Force Life Cycle Management Center (AFLCMC). AFLCMC oversees life cycle management of Air Force weapons systems from inception to retirement. The acquisition lead for the Program Executive Officer for Business Enterprise Systems (PEO-BES) falls under AFMC/CC and will serve as tri-chair for the A4 PB. **(T-1)**

2.4.3.1. Identify funding required to support development, management, and sustainment of CE IT systems. **(T-1)**

2.4.3.2. Advise the AFCEC REAP and/or Roundtable bodies as needed, especially on guidance or issues related to the funding required to support development, management, and sustainment of IT requirements. **(T-1)**

2.4.3.3. Consult with the AFIMSC and AFCEC Data Integration Officers on standards required for CE IT systems. **(T-1)**

2.4.3.4. Ensure assigned CE IT systems compliance with AFI 17-101 and AFI 17-110. **(T-1)**

2.4.3.5. Provide updates to the A4C-2 AO and the AODR on cybersecurity issues of concern for assigned systems. **(T-1)**

2.4.3.6. Conduct testing to remain abreast of security vulnerabilities and ensure testing meets requirements identified by the Security Control Assessor, AODR, and functional users. **(T-1)**

2.4.4. Civil Engineer Security Control Assessor. The Civil Engineer Security Control Assessor resides at AFLCMC/GBZ and will support A4C as the Security Control Assessor for all CE IT Systems and IT Platform on the CE ABL, and performs duties as identified in AFI 17-101. The CE SCA will nominate the Security Control Assessor for CE IT systems on the CE ABL using the Air Force Life Cycle Management Center's Cybersecurity Service Domain for Business Information Systems (AFLCMC/GBZ). **(T-1)**

2.4.5. Commander, Air Force Installation and Mission Support Center (AFIMSC/CC). AFIMSC/CC will be responsible for programming, budgeting, and funding execution of CE IT requirements, to include Program Objective Memorandum (POM) inputs, validation of requirements, and advocacy to ensure continued capacity and capability for the enterprise. **(T-1)**

2.4.6. Headquarters AFIMSC Directorates will:

2.4.6.1. Oversee AFIMSC Enterprise Architecture and guide the implementation of AFIMSC data and technology integration strategy, plans, policy, governance, BEAs, standards, resources, and investments. **(T-1)**

2.4.6.2. Participate in and serve as a voting member of the AFCEC REAP and assist in CE cross functional integration and validation. **(T-1)**

2.4.6.3. Participate in and serve as a core member of the AFCEC Roundtable to provide guidance on

assessments of IT or Data requests. **(T-1)**

2.4.6.4. Bring CE IT requirements generated by AFIMSC forward for review and approval through the Intake and Governance processes detailed in **Chapter 4. (T-1)**

2.4.6.5. Champion validated IT requirements generated by AFIMSC through the BCAC process when necessary. **(T-1)**

2.4.6.6. Coordinate AFIMSC IT strategy documents with A4 CIO and A4C to ensure consistency with overarching strategy, and support development of IT requirements when CE IT acquisitions are under consideration to ensure proposed actions are consistent with SAF/CN policy. **(T-1)**

2.4.6.7. Ensure CE IT systems funded by Operating Agency Code (OAC) 18 are in alignment with mission needs, AF Civil Engineer and USAF vision/goals, strategies, laws, regulations, and policies prior to validating requirements and allocating financial resources. **(T-1)**

2.4.7. AFIMSC Detachments. AFIMSC Detachments will coordinate with AFIMSC and AFCEC/FMO and communicate with MAJCOMs (or USSF equivalent) regarding potential CE Enterprise IT investments or solutions. **(T-1).** AFIMSC Detachments will ensure that investments support the AF vision, provide efficient and effective delivery of capabilities to the warfighter, and maximize ROI to the enterprise while reducing duplication of IT capabilities. **(T-1)**

2.4.8. The Air Force Civil Engineer Center (AFCEC). The Commander, Air Force Civil Engineer Center (AFCEC/CC) will:

2.4.8.1. Provide expert functional recommendations and ensure CE operational-level execution plans are in accordance with policy and in line with CE strategic direction while ensuring proposed installation investment plans align with mission requirements, corporate goals, executive orders, and legislative requirements. **(T-1)**

2.4.8.2. Assign AFCEC/CA to chair the AFCEC REAP. **(T-1).** AFCEC/CC and/or AFCEC/CV will serve as an alternate chair when necessary. **(T-1)**

2.4.8.3. Ensure IT investments are approved by the appropriate IT governance body, utilizing the processes outlined within this DAFGM. **(T-1)**

2.4.9. AFCEC's Functional Management Office (AFCEC/FMO). The AFCEC Functional Management Office (FMO) is aligned under the Business Information Systems and Requirements Directorate (AFCEC/CB) and is responsible for establishing the future vision for CE IT direction based on mission focused strategic drivers and functional capabilities. The FMO identifies opportunities to reduce IT duplication with respect to systems, software, and knowledge management resources, and increase efficiency in alignment with standard CE processes, promoting standardization and consolidation across the enterprise. The FMO will also present fully capitalized IT investments that currently have a non-compliant designation in ITIPS for adjudication through the IT Governance process. The AFCEC FMO is comprised of two divisions: AFCEC/CBS, Business Systems Management, and AFCEC/CBP, Systems Program Development. The FMO performs Functional Lead / Product Owner responsibilities as outlined in DODI 5000.75_DAFI63-144, ensuring strategic goals and objectives are enabled through budgeted, funded, and improved IT delivery. **(T-1)**

AFCEC/FMO will:

2.4.9.1. Chair the AFCEC Roundtable and serve as moderator for the AFCEC REAP. **(T-1)**

2.4.9.2. Inform stakeholders and support development of CE IT related governance, strategy, and policy, and ensure CE IT program alignment with CE IT Strategy. **(T-1)**

2.4.9.3. Notify CE leadership regarding funding shortfalls with fully capitalized investments within the CE IT program, and advocate for resources to support CE IT that are not captured through the annual budget cycle through AFIMSC and the DAF Corporate Structure. **(T-1)**

2.4.9.4. Ensure collaboration between CE functional communities and IT execution by identifying and coordinating the participation of relevant stakeholders and support integration with non-CE IT systems for oversight and reporting within and external to the DAF CE Enterprise. **(T-1)**

2.4.9.5. Review and present an IT Portfolio Request of fully capitalized IT Investments to the AFCEC Roundtable as necessary for adjudication of any areas of non-compliance that must be resolved to prevent loss of capability to the enterprise or impacts to investment funding.

2.4.9.6. Serve as the CE Integration Officer to execute CE Enterprise Data Management per strategic guidance, direction, policy, and governance. Identify and coordinate with data stewards to assess data and support the CE Enterprise with respect to standardization of data elements, improvements to data quality, and analytics.

2.4.9.7. Oversee the collection and management of data across the CE domain. **(T-1)**

2.4.9.8. Oversee the procedures and policies working closely with CE capabilities to collect, prepare, organize, protect, and analyze data assets. **(T-1)**

2.4.9.9. Identify authoritative data sources and data redundancies in conjunction with CE Solution Architects and coordinate authoritative data source approval through the CE Domain Data Representative to ensure consistency across the A4 enterprise in concert with CE IT Governance. **(T-1).**

2.4.9.10 Authoritative data identification must be provided to AFIMSC Principal Data Steward and DAF Chief Data and AI Office (DAF CDAO (SAF/CND)). Data will reside in the approved Data Analytics as a Service (DAaaS) platform. **(T-1)**

2.4.10. AFCEC Functional Directorates. Representatives from AFCEC Functional Directorates will:

2.4.10.1. Identify applicable enterprise CE IT requirements through functional requirements working groups and bring forward to AFCEC/FMO for review, when necessary, as detailed in **Chapter 4**. **(T-1)**

2.4.10.2. Champion IT requirements through the BCAC process. **(T-1)**

2.5. Base Civil Engineers (BCEs). BCEs will:

2.5.1. Bring new enterprise CE IT requirements forward for review and approval through the Governance Structure for CEEG-IT in **Chapter 4**. **(T-1)**

2.5.2. As requirements dictate, nominate personnel to participate in relevant functional requirements validation discussions led by AFCEC/FMO. **(T-2)**

2.5.3. Nominate appropriate personnel to serve as tactical level data stewards for CE IT systems utilized on their installations. **(T-1).** Data stewards will serve as the primary points of contact for the data generated by CE personnel within CE IT systems on their installations. **(T-1)**

Chapter 3
CE ENTERPRISE GOVERNANCE FOR IT (CEEG-IT)

3.1. Governance Structure. Chapter 2, *Stakeholder Roles and Responsibilities* identified organizations within CEEG-IT processes and placed them into the following key groupings: DAF, A4 (to include A4C), AFMC (to include AFIMSC, AFLCMC, and AFCEC), and "Other" stakeholders. These organizations provide oversight, operational support, and decision-making authorities to validate, fund, execute and sustain CE IT Portfolio requirements. CEEG-IT is intended to streamline the CE IT requirements approval process by eliminating redundant reviews, consolidating approval authorities, and only advancing requests to higher governing bodies when necessary.

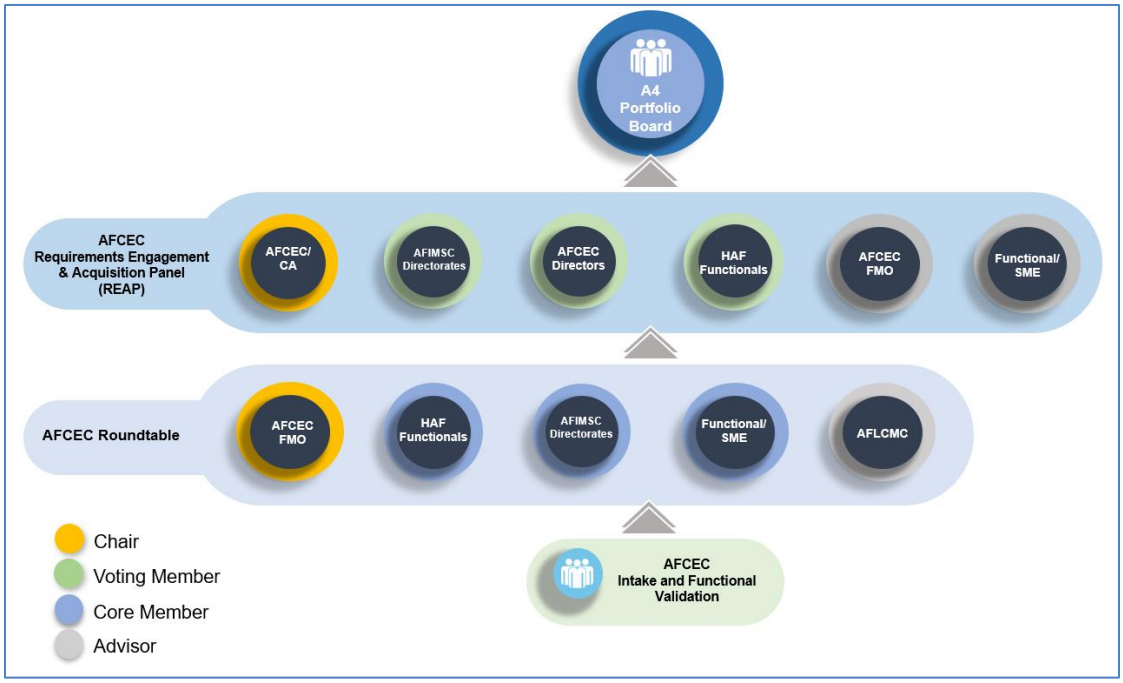

Figure 3.1 Civil Engineer Enterprise Governance for IT Systems

3.2. AFCEC Intake and Functional Validation. When a new CE IT-related request is initiated, the AFCEC/FMO will lead the review, coordination, facilitation, and functional validation of the request through the intake process outlined in **Chapter 4** and detailed within the *CE IT Field Guide*. **(T-1)**

3.2.1. All new requests undergo an initial assessment by the AFCEC/FMO. The AFCEC/FMO will make a recommendation with justification if the request falls under the lifecycle sustainment process and need not be included in the BCAC process. **(T-1)**

3.2.2. Once the request has been validated by this group, it can enter the CEEG-IT process at the next Roundtable. **(T-1)**

3.3. AFCEC Roundtable. The AFCEC Roundtable is AFCEC's operational-level governance group for initial review and vector check of all new CE IT capability requests and CE IT Portfolio investment reviews. **(T-1)**

3.3.1. Request packages will be presented to core members by sponsoring stakeholders with support from AFCEC/FMO. **(T-1)**

3.3.2. For CE IT system investments, all requests at this stage are assessed for validity, completeness,

and approval criteria. The Roundtable will provide a recommended course of action to the AFCEC REAP for the next step in the governance process (advancement, rework, or rejection). **(T-1)**

3.3.3. The AFCEC roundtable will meet quarterly (but may convene more or less frequently as requirements dictate) and is chaired by AFCEC/FMO, with core members including: A4PA, DAF Functionals, A4CS, AFCEC Functionals/Subject Matter Experts (SMEs) and AFIMSC/IZB. **(T-1)**

3.3.4. Additional AFCEC Roundtable personnel may include AFLCMC/GB or SAF/MG as required for appropriate recommendation. **(T-1)**

3.4. The AFCEC Requirements Engagement and Acquisition Panel (REAP). The AFCEC REAP is AFCEC's governance authority for CE IT requirements and data management. **(T-1)**

3.4.1. CE IT requesters with support from AFCEC/FMO will present IT investments or potential IT investments at the AFCEC REAP to be voted on by core voting AFCEC REAP members. All requests presented to the AFCEC REAP for decision are required to have met with one or more operational groups for applicable review and adjudication and must present relevant solution analysis documentation in alignment with BCAC, including a concise business problem with desired end state, documented LRPs, alignment with BEA, and potential capability performance measures. AFCEC/CD or AFCEC/CV will chair the AFCEC REAP panel.

3.4.2. AFIMSC/IZB is responsible for validating program, budget, and fund execution for IT requirements vetted by CE or A4 IT governance as appropriate to ensure continued capacity and capability for the enterprise. **(T-1)**

3.4.3. Voting members of the AFCEC REAP include AFCEC/CA, AFIMSC/IZB, AFCEC Directors and the HAF Functionals. **(T-1)**

3.4.4. Non-voting advisory members of the AFCEC REAP include AFCEC/FMO, AF/A4PA, and the AFCEC Functionals/SMEs as required. The output of the AFCEC REAP will be provided to the AFIMSC IT Requirements Board for funding and/or A4 PB for BCAC process as necessary. **(T-1)**

3.4.5. AFIMSC Portfolio Management (AFIMSC/IZBO) allocates resources, as available, to CE IT functional and system requirements that have been vetted by CE and/or A4 IT governance as appropriate. **(T-1)**

3.4.6. AFIMSC/IZB is responsible for programming, budgeting, and funding execution of CE IT requirements, to include POM inputs, validation of requirements, and advocacy to ensure continued capacity and capability for the enterprise. **(T-1)**

3.5. The A4 Portfolio Board (A4PB). BCAC Authority to Proceed (ATP) decisions for BCAC ATPs 1, 2, 3 and 4 are evaluated by the A4 PB with ATP 1 decisions made by SAF/MG, ATP 3 and 4 decisions made by the Milestone Decision Authority, and ATP 2 decisions made by both SAF/MG and the Milestone Decision Authority, as identified in DoDI 5000.75_DAFI63-144. Following BCAC ensures a PMO is assigned and supports review for alignment to appropriate AO Authorization Boundary, among other determinations as identified per request. **(T-1)**

3.5.1. Request packages submitted to the A4 PB will be presented to the Board by sponsoring stakeholders with support from AFCEC/FMO. **(T-1)**

3.5.2. AF/A4P, SAF/MG, and PEO-BES chair the board with support from topic-based advisory members including representatives from: AF/A4P, AFLCMC/GB, SAF/MG, AF/A4C, AF/A4L, AF/A4S, AFMC/A4/10, SAF/CN, SAF/FMF, SAF/CND (DAF CDAO), AFMC/FM, AFSC/LG, SAF/AQI, AFIMSC/CA, PEO C3I&N, AFLCMC/LG-LZ, SAF/AQD, and SAF/AQR. **(T-1)**

Chapter 4
CE IT REQUIREMENTS INTAKE PROCESS

4.1. Introduction. The CEEG-IT process is intended to evaluate, resource, approve and deploy CE IT requirements in a streamlined manner. During the intake process, CE IT requirements are vetted in parallel against the following criteria: alignment with strategic goals, CE enterprise architecture, performance targets, elimination of duplicative programs, cybersecurity risk management, cost optimization, compliance with applicable legal, regulatory, and policy requirements, improved communication or training with stakeholders, and appropriate utilization of authoritative data sources. The AFCEC/FMO coordinates with CE Functionals and SMEs and utilizes input based on their areas of expertise to evaluate all incoming requests. This ability to review, collaborate, and aggregate input gives the CE Community a single point of entry into the CEEG-IT process and will expedite CE IT requirements approval.

4.2. Intake Process Overview for CE IT Requirements. At intake, the CE Community will submit CE IT requirements directly to AFCEC/FMO, who will coordinate with both Functionals and SMEs to validate requests against the criteria listed above and provide a completed CE IT requirements request to the governance groups for action. For example, AFIMSC IT Requirements Board for software/EPL requirements and AFCEC Roundtable for CE Enterprise IT System investments. **(T-1)**

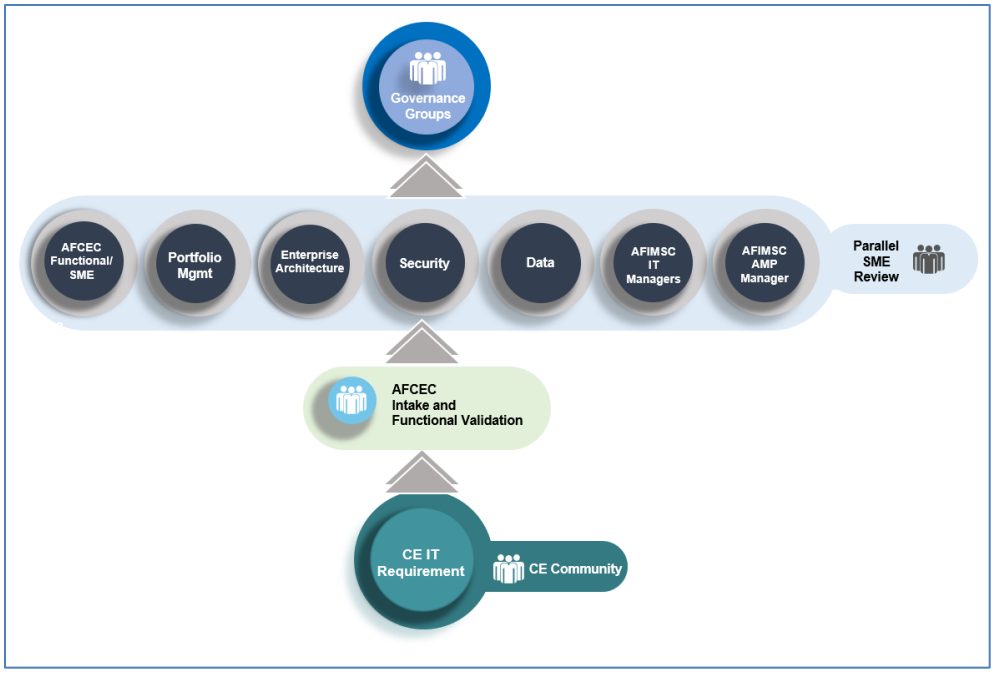

Figure 4.2 CE IT Requirements Intake Process

4.2.1. Request Initiation. If a need for a new CE IT capability and/or investment is identified, the requirement owner will initiate the request with the AFCEC/FMO. **(T-1)**

4.2.1.1. Enhancement Requirements. Requests for enhancement to an existing IT capability will first flow through CE IT Functional Requirements Working Groups (FRWGs) **(T-2).**

4.2.1.2. Enhancement Requests must be initiated through that CE IT systems Functional SME. **(T-2).**

4.2.1.3. Each existing CE IT system has an established FRWG, which acts as a platform for identifying and prioritizing system sustainment requirements for each IT systems product backlog. Each IT system's FRWG has the responsibility to identify when a requirement is not within the scope of

sustainment and requires further evaluation to identify the appropriate path to execution. FRWGs will input out of scope enhancement requests to AFCEC/FMO and the CEEG-IT for further evaluation when necessary. Additional information on how to enter requests for enhancements to existing CE IT systems into the CEEG-IT process can be found in the *CE IT Field Guide*. **(T-2)**

4.2.1.4. Lifecycle Sustainment Requirements: Sustainment requirements flow through CE IT FRWGs for review, approval, prioritization, and eventual joint-grooming with AFLCMC for integration into system product roadmaps for eventual execution. **(T-2)**

4.2.1.5. Authority for sustainment requirements resides with the IT Systems Program Manager & Functional Lead. **(T-1)**

4.2.1.6. IT Innovation and Pilot Project Efforts. The handling of IT innovation and/or pilot project efforts differ from lifecycle sustainment and enhancement requirements, or requests to acquire a new IT capability. Innovation and/or pilot efforts might include IT, with CE specific application that is not yet tested, approved and/or acquired. Innovation and/or pilot efforts are often initiated at the installation level and promoted upward to functional program offices to consider for wider adoption and deployment. While these innovation projects may satisfy a localized need, not all fulfill an enterprise-wide requirement. Furthermore, innovation and/or pilot efforts are intended to undergo a form of rapid acquisition to shorten the time required to develop and test a prototype. To promote local innovation and the testing of new ideas and prototypes through these pilot efforts, CE IT innovation and/or pilot projects do not formally process through the CEEG-IT. Local efforts at prototyping and testing may need to be coordinated through SAF/A4 IT portfolio managers or SAF/MG portfolio reviews IAW AFI 17-110 for duplicative features and integration with the overall enterprise. **(T-2)**

4.2.1.6.1. All innovation and/or pilot efforts that include an IT component will require an ATO and/or IATT to utilize and/or collect data used by the DoD, or to connect to DoD networks. Requests for ATO or IATT will require A&A as outlined within the *Risk Management Framework (RMF)*. A&A requirements for CE IT and Platform capabilities are outlined in the *A4 CIO A&A Guide*. Functional sponsorship, funding for the innovation and/or pilot, sustainment of the system in production, and cybersecurity resources on-hand to test and monitor the cybersecurity posture of the system are required to be accepted into the CE IT and Platforms AO Boundary.

4.2.1.6.2. AFCEC's Innovation Cell (AFCEC/CBI) will assist IT innovation proponents by facilitating a parallel review with AFCEC/FMO to ensure pre-requisite A&A requirements are satisfied. **(T-2)**

4.2.1.6.3. Once A&A requirements are complete, the Innovation Cell may continue to guide the proponent in staffing an ATO or IATT request to A4CS for CE Boundary AO approval. **(T-2)**

4.2.1.7. New IT Capability Requests (ITCRs). AFCEC/FMO serves as the input source for newly identified CE IT requirements. **(T-1)**

4.2.1.7.1. If a requirement for a new capability is identified, an IT Capability Request (ITCR) can be initiated via the *CE IT Request Tracker Portal:* https://usaf.dps.mil/sites/CEPortal1/CEIT/CEITRequestTracker/Lists/CEITRequests/NewForm.aspx?Source=/sites/CEPortal1/CEIT/CEITRequestTracker/SitePages/MyRequests.aspx&RootFolder=/sites/CEPortal1/CEIT/CEITRequestTracker/Lists/CEITRequests

4.2.1.7.2. A new CE IT capability request generated by AFIMSC, AFCEC, ANG or AFRC must be functionally sponsored by an appointed representative from the requesting organization while proceeding through the BCAC process. **(T-1)**

4.2.1.7.3. Per DODI 5000.75_DAFI63-144, the functional sponsor is the DoD or Component senior leader with business function responsibility seeking to improve mission performance. The functional sponsor confirms the need for improved business operations and represents the user community interests throughout the BCAC. **(T-1)**

4.2.2. Functional Validation. The AFCEC/FMO, NGB/A4, or AFRC/A4 staff, as appropriate, will review, coordinate, facilitate, and secure functional validation for CE capability requests. **(T-1)**

4.2.2.1. They will also make a recommendation with justification if the request falls under the life cycle sustainment process and does not need to enter the BCAC process. **(T-1)**

4.2.2.2. AFCEC Functionals/SMEs and the AFCEC/FMO Portfolio Management, Enterprise Architecture, Enterprise Data Management, Cybersecurity, and IT Acquisition teams will assist in determining the validity and completeness of all CE IT requirement requests. **(T-1).**

4.2.2.3. While dependent upon quality of the submission and requestor involvement, AFCEC Functionals/SMEs conducting reviews of CE IT requirement requests will provide questions, input, or recommendations back to FMO Intake within five business days of receipt. **(T-2).**

4.2.2.4. Exceptions to this timeline may be coordinated between Functional SMEs and AFCEC/FMO on a case-by-case basis. **(T-2)**

4.2.2.5. Once approved by the appropriate AF, NGB or AFRC forum, a request package can officially move forward to the AFCEC Roundtable, the first operational forum in the CE Enterprise Governance process. **(T-1)**

4.2.3. CE IT Governance Groups. Upon completion of parallel SME reviews and aggregation of input, a finalized CE IT requirements package will be prepared by AFCEC/FMO within 10 business days to officially complete the intake process. **(T-2)**

4.2.3.1. Exceptions to this timeline may be coordinated between Functional SMEs and AFCEC/FMO on a case-by-case basis. **(T-2)**

4.2.3.2. The CE IT requirements package (i.e., IT Request Form, Problem Statement, Quad Chart, supporting documentation) will be submitted to the AFCEC Roundtable as the entry point to the CEEG-IT outlined in **Chapter 3**. Additional detail on content of CE IT Requirement Request Packages can be found within the *CE IT Field Guide*. **(T-1)**

4.2.4. Capability is Budgeted, Funded, and Resourced for Execution. After receiving appropriate decisional board approval, new capability or lifecycle sustainment requests that do not need to be submitted for BCAC authorization must be budgeted, funded, and resourced within the proper AFIMSC Portfolio. **(T-1)**

4.2.4.1. This includes validation of requirements, POM inputs, and advocacy to ensure continued capacity and capability for the enterprise.

4.2.4.2. If the requirement is to be executed in the year of execution, then AFCEC/FMO will advocate for resources through the existing Un-Funded Requirement (UFR) request process. **(T-1)**

4.2.4.3. If the requirement is to be executed in future year programs, then AFCEC/FMO will coordinate with AFIMSC Portfolio Management (AFIMSC/IZB) to develop a resourcing plan. **(T-1)**

4.2.4.4. AFCEC/FMO will coordinate the request archival process at the AFCEC Roundtable once a resourcing plan has been approved by AFIMSC. **(T-1)**

4.2.4.5. AFIMSC/IZB allocates resources to CE IT functional and system requirements that have been vetted at the AFCEC REAP and approved at the A4 PB. **(T-1)**

4.2.4.6. AFIMSC/IZB is responsible for programming, budgeting, and funding execution of CE IT requirements, to include POM inputs, validation of requirements, and advocacy to ensure continued capacity and capability for the enterprise. **(T-1)**

4.3. Guidance for Non-BMA Systems. The following section describes special guidance procedures for Warfighting Mission Area Systems and Defense Intelligence Mission Area Systems. Both subjects require specific governance coordination, which is outlined below.

4.3.1. Special Guidance for Warfighting Mission Area Systems. For Warfighter Mission Areas systems, follow the above governance approval process until reaching the A4 PB. After a system is reviewed at the A4 PB, the approval process leaves the CEEG-IT governance process and enters a separate DAF Joint Capabilities Integration and Development System (JCIDS) governance process. This process is detailed in the *AF/A5R Requirements Development Guidebook*. The A5R website also

provides an orientation briefing for the DAF JCIDS process. **(T-1)**

4.3.2. Special Guidance for Defense Intelligence Mission Area Systems. For Defense Intelligence Mission Area (DIMA) systems, follow the above governance approval process until reaching the A4 PB. **(T-1)**

4.3.2.1. At that time, the approval process leaves the CEEG-IT governance process and enters a separate Air Force and Joint governance process. The Explosive Ordnance Disposal Information Management System (EODIMS) program, for example, has been categorized as a DIMA system. EODIMS follows an established, chartered Joint Configuration Control Board (JCCB) process, for requirements approval. JCCB members are the action officers to the DoD Explosive Ordnance Disposal Program Board representing the General and Flag Officers from each Service with AFCEC/CXD functioning as the permanent EODIMS chair **(T-1)**

4.3.2.2. Requirements approved at the EODIMS JCCB are presented to the CEEG-IT governance process for awareness; DAF-only requirements will follow CE governance approval process. **(T-1)**

Attachment A

References, Prescribed Forms, Adopted Forms, Abbreviations, Acronyms, and Definitions

References

DAFI 90-160, *Publications and Forms Management,* updated 14 April 2022. https://static.e-publishing.af.mil/production/1/saf_aa/publication/dafi90-160/dafi90-160.pdf

DAFGM 2022-32-01, *Civil Engineer Control Systems Cybersecurity*, published 10 March 2022. https://static.e-publishing.af.mil/production/1/af_a4/publication/dafgm2022-32-01/dafgm2022-32-01.pdf

HAFMD 1-18, *Assistant Secretary of the Air Force (Installations, Environment and Energy)*, 10 July 2014. https://static.e-publishing.af.mil/production/1/saf_ie/publication/hafmd1-18/hafmd1-18.pdf

HAFMD 1-38, *Deputy Chief of Staff (Logistics, Engineering and Force Protection)*, updated 21 June 2021. https://static.e-publishing.af.mil/production/1/af_a4/publication/hafmd1-38/hafmd1-38_.pdf

CE IT Request Tracker Portal. https://usaf.dps.mil/sites/CEPortal1/CEIT/CEITRequestTracker/Lists/CEITRequests/NewForm.aspx?Source=/sites/CEPortal1/CEIT/CEITRequestTracker/SitePages/MyRequests.aspx&RootFolder=/sites/CEPortal1/CEIT/CEITRequestTracker/Lists/CEITRequests

CE IT Field Guide, Version 4.1. 02 September 2022. https://usaf.dps.mil/sites/CEPortal1/CEIT/CEITRequestTracker/CEITRequestTemplates/AF%20CE%20IT%20Field%20Guide.pdf

AFI 33-322, *Records Management and Information Governance Program*, 23 March 2020. https://static.e-publishing.af.mil/production/1/saf_cn/publication/afi33-322/afi33-322.pdf

AFI 63-101_20-101, *Integrated Life Cycle Management,* updated 30 June 2020. https://static.e-publishing.af.mil/production/1/saf_aq/publication/afi63-101_20-101/afi63-101_20-101.pdf

AFI 17-110, *Information Technology Portfolio Management and Capital Planning and Investment Control,* 23 May 2018. https://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-110/afi17-110.pdf

AFI 17-101, *Risk Management Framework (RMF) For Air Force Information Technology (IT),* 6 February 2020. https://static.e-publishing.af.mil/production/1/saf_cn/publication/afi17-101/afi17-101.pdf

AFI 17-140, *Architecting*, 29 June 2018. https://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-140/afi17-140.pdf

AFI 63-138, *Acquisition of Services,* 30 September 2019. https://static.e-publishing.af.mil/production/1/saf_aq/publication/afi63-138/afi63-138.pdf

AF/A5R Requirements Development Guidebook, 5 December 2019. Log into AF Portal and then access the following link: https://www.my.af.mil/gcss-af/USAF/ep/globalTab.do?channelPageId=s6925EC1352150FB5E044080020E329A9

DAFMAN 17-1203, *Information Technology (IT) Asset Management (ITAM)*, updated 13 September 2022. https://static.e-publishing.af.mil/production/1/saf_cn/publication/dafman17-1203/afman17-1203.pdf

DAFMAN 90-161, *Publishing Processes and Procedures.* 15 April 2022. https://static.e-publishing.af.mil/production/1/saf_aa/publication/dafman90-161/dafman90-161.pdf

DAFI 32-101-12, *Installation Geospatial Information and Services (Installation GI&S)*, 21 February 2023. https://static.e-publishing.af.mil/production/1/af_a4/publication/dafi32-10112/dafi32-10112.pdf

Air Force Installation and Mission Support Center, ExPlan Guidance, updated 29 July 2021. https://usaf.dps.mil/teams/13569/izbstratcomm/SitePages/Home.aspx?RootFolder=%2Fteams%2F13569%2Fizbstratcomm%2FShared%20Documents%2F2%20%2D%20Library&FolderCTID=0x01200006626BF444F7AF4E8A28006A3EE53CA1&View=%7BB0C9FD1E%2D3E35%2D4F7C%2D8F93%2D0179D7D53F4E%7D

DoDI 8115.02, *Information Technology Portfolio Management Implementation*, updated 30 October 2006. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/811502p.pdf#:~:text=DoDI%208115.02%2C%20October%2030%2C%202006%202%202.1.2.%20The,DoD%20mission%20areas%20established%20to%20manage%20IT%20portfolios.

DoDI 5000.75 DAFI63-144, *Business Systems Requirements and Acquisitions*, 23 January 2023. https://static.e-publishing.af.mil/production/1/saf_aq/publication/dodi5000.75_dafi63-144/dodi5000.75_dafi63-144.pdf

DoDD 8000.01, *Management of the Department of Defense Information Enterprise (DoD IE)*, updated 27 July 2017. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/800001p.pdf

OMB Circular A-130; *Managing Information as a Strategic Resource*, 28 July 2016. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

AFPD 10-6, *Operational Capability Requirements Development*, 6 November 2013. https://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-601/afi10-601.pdf

DAF Implementation Plan to the DoD Data Strategy, February 2021, https://usaf.dps.mil/:b:/s/13057/CND/EbCTzSwjz7BGrHT1H05rwPEB2duAujyssqiFE1JfoF458Q?e=ZPyOEG
Management Plan 3.0 for Air Force Civil Engineer Center (AFCEC), October 2022. https://portal.afcec.hedc.af.mil/dashboard/Shared%20Documents/Final%20Management%20Plan%203.0%2020%20Oct%2022.pdf

AF/A4 Data Stewardship Framework, 01 December 2020. https://usaf.dps.mil/teams/AF-A4/A4P/A4_CIO/External%20to%20A4/Forms/AllItems.aspx?id=%2Fteams%2FAF%2DA4%2FA4P%2FA4%5FCIO%2FExternal%20to%20A4%2FA4%2FCurrent%2FA4%20Data%20Stewardship%20Framework%201%20Dec%202020%2Epdf&viewid=2b71104f%2Dfa85%2D448e%2D8f75%2D18ada65fcb11&parent=%2Fteams%2FAF%2DA4%2FA4P%2FA4%5FCIO%2FExternal%20to%20A4%2FA4%2FCurrent

AF/A4 Enterprise Architecture (EA) Framework, 16 March 2021. https://usaf.dps.mil/teams/AF-A4/A4P/A4_CIO/Architecture Development/Forms/AllItems.aspx?id=%2Fteams%2FAF-A4%2FA4P%2FA4_CIO%2FArchitecture Development%2FEA Governance%2FA4 EA Framework %2816 Mar 2021%29 Signed%2Epdf&parent=%2Fteams%2FAF-A4%2FA4P%2FA4_CIO%2FArchitecture Development%2FEA Governance

AF/A4 Chief Information Officer Assessment and Authorization Guide, 04 September 2020. https://usaf.dps.mil/teams/AF-A4/A4P/A4PA/ELITandMgtServices/CybersecurityGovernance/Shared%20Documents/A4%20CIO%20Assessment%20and%20Authorization%20Guide%20(2020).pdf

Prescribed Forms

None

Adopted Forms

DAF Form 847, *Recommendation for Change of Publication.* https://static.e-publishing.af.mil/production/1/saf_aa/form/daf847/daf847.pdf

Abbreviations and Acronyms

A&A – Assessment and Authorization

ABL – Authorized Boundary List

AF – Air Force

AFCEC – Air Force Civil Engineer Center

AFGM – Air Force Guidance Memorandum

AFI – Air Force Instruction

AFIMSC – Air Force Installation & Mission Support Center

AFLCMC – Air Force Life Cycle Management Center

AFMAN – Air Force Manual

AFRC – Air Force Reserve Command

ANG – Air National Guard

AO – Authorizing Official

AODR – Authorizing Official Designated Representative

ATO – Authority to Operate

ATP – Authority to Proceed

BCAC – Business Capability Acquisition Cycle

BEA – Business Enterprise Architectures

BMA – Business Mission Area

CE – Civil Engineer

CEEG-IT – Civil Engineer Enterprise Governance for Information Technology

DAF – Department of Air Force

DAFGM – Department of Air Force Guidance Memorandum

DAFI – Department of Air Force Instruction

DIMA – Defense Intelligence Mission Area

DoDI – Department of Defense Instruction

EOD – Explosive Ordnance Disposal

EODIMS – Explosive Ordnance Disposal Information Management System

FMO – Functional Management Office

FRWG – Functional Requirements Working Group

HAF – Headquarters Air Force

HAFMD – Headquarters Air Force Mission Directive

IATT – Interim Authority to Test

IT – Information Technology

LEFP – Logistics, Engineering, and Force Protection

MAJCOM – Major Command

NGB – National Guard Bureau

NIST – National Institute of Standards and Technology

PEC – Program Element Code

REAP – Requirements Engagement and Acquisition Panel

RMF – Risk Management Framework

USAF – United States Air Force

Definitions

Authorization — Access privileges granted to a user, program, or process or the act of granting those privileges.

Authorization Boundary — All components of an information system to be authorized for operation by an AO. This excludes separately authorized systems to which the information system is connected.

Authorizing Official (AO) — A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Authorizing Official Designated Representative (AODR) — An organizational official acting on behalf of an AO in carrying out and coordinating the required activities associated with security authorization.

Business Mission Area (BMA)—The Business Mission Area ensures the right capabilities, resources, and materiel are reliably delivered to our warfighters: what they need, where they need it, when they need it, anywhere in the world. To cost-effectively meet these requirements, the Department of Defense current business and financial management infrastructure - processes, systems, and data standards - are being transformed to ensure better support to the warfighter and improve accountability to the taxpayer. Integration of business transformation for the Department of Defense business enterprise is led by the Deputy Secretary of Defense in their role as the Chief Operating Officer of the Department.

Business Capability—A business capability is the articulation of the core abilities or functions the organization needs to deliver requisite products and services to provide value for the business and its constituents.

Business Capability Acquisition Cycle—The Air Force execution of the business system capability acquisition process required in DoDI 5000.75_DAFI63-144, *Business Systems Requirements and Acquisition*.

Business Mission Area (BMA) System—Business systems are defined as information systems operated by,

for, or on behalf of the Department of Defense, including financial systems, financial data feeder systems, contracting systems, logistics systems, planning and budgeting systems, installations management systems, human resources management systems, and training and readiness systems. A business system does not include a national security system, or an information system used exclusively by and within the defense commissary system or the exchange system or other instrumentality of the Department of Defense conducted for the morale, welfare, and recreation of members of the armed forces using non-appropriated funds. This AFGM uses Business System interchangeably with Defense Business System.

Capability Request —Reference to formal initiation a new business capability request via the CE IT Request Tracker Portal. To complete a capability request, the following required fields will need to be completed: Requestor Name/Org/Contact Info, Project Manager Name/Org/Contact Info, Sponsor Name/Org/Contact Info, Request Title, Need By Date, Functional Lead, Strategic Driver, Operational Level, Capability Need Description, Capability Benefits Description, Return on Investment, Regulatory Mandates, Proof of Standardization Requirements Met, Proof of IT Security Risk Reduction, Proof of Planning and Informed Decisions, Technical Constraints Description, Listing of Similar IT Capabilities that would Fulfill a Partial Need, COTS vs GOTS Solution, Investment Type, Lifecycle Phase, Confidentiality Level, and Priority.

Control System (CS) —A system in which deliberate guidance or manipulation is used to achieve a prescribed value for a variable. Control systems include SCADA, DCS, PLCs and other types of industrial measurement and control systems. See DAFGM2022-32-01, *Civil Engineer Control Systems Cybersecurity*.

Cybersecurity—Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. See DAFGM2022-32-01, *Civil Engineer Control Systems Cybersecurity*.

Data Domain Representative—Appointed by their functional communities and approved by the A4 Data Officer. They are accountable for the quality of the data, metadata, and the data culture within their functional domain.

Data Integration Officer—Appointed by the A4 Chief Information Officer and is tasked with ensuring A4 data is defined and managed from an enterprise perspective. The A4 Data Officer's primary responsibility is to ensure that data assets are valued as enterprise assets instead of as the sole property of any organization.

Decision Authority—The decision authority is the individual responsible for leading the decision-making process for the current phase of BCAC. The decision authority collects input from all pertinent stakeholders and makes final decisions. DoDI 5000.75, Table 3 identifies the Decision Authority based upon the Authority to Proceed.

Defense Business System—Business systems are defined by 10 United States Code § 2222 as information systems operated by, for, or on behalf of the Department of Defense, including: financial systems, financial data feeder systems, contracting systems, logistics systems, planning and budgeting systems, installations management systems, human resources management systems, and training and readiness systems. A business system does not include a national security system, or an information system used exclusively by and within the defense commissary system or the exchange system or other instrumentality of the Department of Defense conducted for the morale, welfare, and recreation of members of the armed forces using non-appropriated funds. This DAFGM uses Defense Business System interchangeably with Business System.

Defense Intelligence Mission Area System –- See DoDI 8115.02, *Information Technology Portfolio Management Implementation.* The DIMA includes IT investments within the Military Intelligence Program and Defense component programs of the National Intelligence Program. The USD(I) has delegated responsibility for managing the DIMA portfolio to the Director, Defense Intelligence Agency, but USD(I) retains final signature authority. DIMA management will require coordination of issues among portfolios that

extend beyond the DoD to the overall Intelligence Community.

Domain Data Steward—A Domain Data Steward represents their respective community in AF/A4 data governance. They provide subject matter expertise in the context of mission execution and are accountable for the master data, compliance with data management policies, procedures and data standards within a sub-domain.

Information System— (DoD Directive 8000.01, *Management of the Department of Defense Information Enterprise*). A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information Technology (IT)—In accordance with Office of Management and Budget Circular A-130, DoD Directive 8000.01, and NIST, FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems, 2006, the term "information technology" is defined as: "Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. This includes if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use of that equipment, or of that equipment to a significant extent in the performance of a service or the furnishing of a product. IT includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources, but does not include any equipment acquired by a federal contractor incidental to a federal contract."

IT can also refer to computing and/or communications hardware and/or software components and related resources that can collect, store, process, maintain, share, transmit, or dispose of data. IT components include computers and associated peripheral devices, computer operating systems, utility/support software, and communications hardware and software.

IT Platforms—A computer or hardware device and/or associated operating system, or a virtual environment, on which software can be installed or run (NIST, Common Platform Enumeration: Naming Specification Version 2.3, 2011).

IT Portfolio Management— See DoDI 8115.02, *Information Technology Portfolio Management Implementation.* The management of selected groupings of Information Technology investments using strategic planning, architectures, and outcome-based performance measures to achieve a mission capability. Outcome-based performance measures are addressed through meeting Capital Planning and Investment Control execution requirements.

Milestone Decision Authority—Approves critical acquisition decisions for the Authority-to-Proceed decision points or concurs in contractual commitments. The Milestone Decision Authority is the decision authority for the development and delivery of business systems within related cost, schedule, and performance parameters. DoDI 5000.75_DAFI63-144, Table 1 identifies the Milestone Decision Authority based on the business system category.

Risk—A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Risk Management — The program and supporting processes to manage information security risk to

organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.

Risk Management Framework — A structured approach used to oversee and manage risk for an enterprise.

Security — A condition resulting from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.

Security Controls — The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Security Control Assessment — The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Sponsor (Joint Capabilities Integration and Development System)—Per the Air Force Requirements Development Guidebook Vol 1, 19 Sep 2016, sponsors will lead the actual development of operational capability requirements and associated documentation for their assigned systems, programs, functions and/or missions. This is typically the Lead Command (or equivalent) for the mission area or program. Sponsors use formal capabilities-based processes to identify, evaluate, develop, field, and sustain capabilities competing for limited resources. The intent of these processes is to facilitate timely development of affordable and sustainable operational systems needed by warfighters and combatant commanders. Specific Sponsor roles and responsibilities are detailed in AFPD 10-6, *Operational Capability Requirements Development*.

Attachment B

Parameters of CE IT and Resources for Information on Other Technology Topics

Parameters of CE IT

Topic	Category	Recommended Reference
CE Enterprise IT System / Software Development / Sustainment *Includes AFGIMS Systems Software Management / Sustainment*	CE IT	This DAFGM and the *Air Force Civil Engineer Information Technology Field Guide*. https://usaf.dps.mil/teams/10041/dashboards/ce%20it%20requests%20references/af%20ce%20it%20field%20guide.pdf AFI 17-110, *Information Technology Portfolio Management and Capital Planning and Investment Control*. https://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-110/afi17-110.pdf DAFMAN 17-1203, *Information Technology (IT) Asset Management (ITAM)*. https://static.e-publishing.af.mil/production/1/saf_cn/publication/dafman17-1203/afman17-1203.pdf For AFGIMS guidance, see also AFI 32-101-12, *Installation Geospatial Information and Services (Installation GI&S)*. https://static.e-publishing.af.mil/production/1/af_a4/publication/dafi32-10112/dafi32-10112.pdf

Resources for Information on Other Technology Topics

Topic	Category	Recommended Reference
Geospatial Software	IGI&S	Additional AFIMSC information. Including ExPlan Guidance, CE IT Investment Matrix and EEIC Map files. https://usaf.dps.mil/teams/13569/izbstratcomm/SitePages/Home.aspx?RootFolder=%2Fteams%2F13569%2Fizbstratcomm%2FShared%20Documents%2F2%20%2D%20Library&FolderCTID=0x01200006626BF444F7AF4E8A28006A3EE53CA1&View=%7BB0C9FD1E%2D3E35%2D4F7C%2D8F93%2D0179D7D53F4E%7D
COTS Software Purchases IT Hardware Purchase / Maintenance Imagery Acquisition, Spatial Data Collection / Maintenance, Non-	IT Asset Management	AFI 17-110, *Information Technology Portfolio Management and Capital Planning and Investment Control*. https://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi17-110/afi17-110.pdf

Spatial Data Collection / Maintenance		DAFMAN 17-1203, *Information Technology (IT) Asset Management (ITAM).* https://static.e-publishing.af.mil/production/1/saf_cn/publication/dafman17-1203/afman17-1203.pdf Additional AFIMSC information. Including ExPlan Guidance, CE IT Investment Matrix and EEIC Map files. https://usaf.dps.mil/teams/13569/izbstratcomm/SitePages/Home.aspx?RootFolder=%2Fteams%2F13569%2Fizbstratcomm%2FShared%20Documents%2F2%20%2D%20Library&FolderCTID=0x012000006626BF444F7AF4E8A28006A3EE53CA1&View=%7BB0C9FD1E%2D3E35%2D4F7C%2D8F93%2D0179D7D53F4E%7D
Control Systems Cybersecurity *Includes: Fire Detection Systems Hardware, Fire Detection Systems Software / Data Acquisition (e.g., Monaco), Data from Industrial Control Systems / Facility Related Control Systems*	OT	UFC 4-010-06, *Cybersecurity of Facility-Related Controls Systems*. https://www.wbdg.org/FFC/DOD/UFC/ufc_4_010_06_2016_c1.pdf