

**BY ORDER OF THE COMMANDER
AIR FORCE MATERIEL COMMAND**

**AIR FORCE MATERIEL COMMAND
INSTRUCTION 33-108**



29 MAY 2014

Incorporating Change 1, 10 NOVEMBER 2016

Communications and Information

***AFMC LIFE CYCLE INFORMATION
TECHNOLOGY GOVERNANCE***

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication

OPR: HQ AFMC/A6IC

Certified by: HQ AFMC/A61
(Ms. Sharon Bias)

Supersedes: AFMCPD33-4,
22 November 2005

Pages: 22

This instruction establishes Air Force Materiel Command (AFMC) guidance in conjunction with AFPD 17-1, *Information Dominance Governance and Management*; AFI 33-141, *Air Force Information Technology Portfolio Management and IT Investment Review*. This instruction implements guidance from 44 United States Code (USC) **Chapter 35**, *Coordination Of Federal Information Policy*; 40 USC Subtitle III, *Information Technology Management (Clinger-Cohen Act (CCA))*; 10 USC § 2222, *Defense Business systems: Architecture, Accountability, and Modernization*; 10 USC § 2223, *Information Technology: Additional Responsibilities of Chief Information Officers*; 10 USC § 2223a, *Information Technology Acquisition Planning and Oversight Requirements*; Executive Order 13011, *Federal Information Technology*, Office of Management and Budget (OMB) Circular A-11, *Preparation, Submission and Execution of the Budget*; OMB Circular A-130, *Management of Federal Information Resources*; DoD Financial Management Regulation 7000.14-R, Volume 2B; DoDD 8115.01, *Information Technology Portfolio Management*; DoDI 8115.02, *Information Technology Portfolio Management*; AFI 33-150, *Management of Cyberspace Support Activities*; and AFMCI 90-601, *AFMC Corporate Structure*. This instruction applies to all AFMC units. This instruction develops the scope, responsibilities, membership and processes for implementing and executing the AFMC Information Technology (IT) Investments. This instruction establishes a management framework to develop AFMC's IT Investment portfolio for decision making across the command and in support of the Headquarters Air Force (HAF) and Secretary of the Air Force (SAF) functional staffs. This instruction does not apply to the Air National Guard or Air Force Reserve units and members. This publication may be supplemented at any level, but all direct

supplements must be routed to the Office of Primary Responsibility (OPR) of this publication for coordination before certification and approval. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional 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 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. 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).

SUMMARY OF CHANGES

This interim change revises AFMCI33-108 by changing OPR Office symbol throughout the document, updating the opening paragraph and replacing Attachment 1. A margin bar (|) indicates newly revised material.

1.	Purpose.....	2
Figure 1.	IT Portfolio Management Decision Support Interactions DoDI 8115 02.	5
2.	Roles:	7
Figure 2.	IT Investment Mission Area Mapping to Roles.....	7
3.	Responsibilities:.....	11
Figure 3.	IT Portfolio Structure AFMC Assignment.....	12
4.	AFMC IT PfM Processes and Governance Structure:	15
Figure 4.	AFMC IT Governance Structure.	16
Attachment 1— GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION		18
Attachment 2— BREAKOUT FROM JCA OF WMA-CMS		21

1. Purpose. In order to effectively and efficiently comply with AFI 33-141, USC and Executive Order 13011, AFMC must provide centralized planning and governance of AFMC’s IT investments. The intent of this instruction is to consolidate current workload. AFI 33-141 delegates IT Portfolio Management (PfM) Owner responsibility to the MAJCOM CV for IT investments funded within the MAJCOM. Per USC, Chief Information Officers (CIOs) must monitor the performance of IT investments, evaluate their effectiveness and recommend whether to continue, modify, or terminate individual IT investments. As a result, the AFMC CIO must not only control Command IT investments, but also comply with AF functional leads and

AF/DoD CIO's policies and decisions resulting from these mandates. This instruction defines the AFMC policy and actions required to ensure compliance with the governing requirements and higher-level guidance. This policy assigns roles and responsibilities on how AFMC will analyze, select, control, and evaluate its AFMC IT investments. See Attachment 1 for a glossary of references and supporting information.

1.1. Policy Statement. This AFMCI ensures the IT PfM processes within AFMC (Mission Area and Center levels) are established to provide oversight to choose IT investments based on a standard scoring and reporting mechanism designed to reduce duplicate and overlapping capabilities. AFMC IT planning and investment governance is executed through the IT PfM processes. IT investments will play a key role in the automation and integration of AFMC's processes. Thus, a close working relationship between current capabilities, capabilities required, process reengineering and IT modernization efforts are critical as we move forward. USC requires all Federal agencies to conduct IT investment management in such a way as to ensure that both mission-related processes and administrative processes effectively and efficiently utilize IT. All IT investments are to be assessed in terms of cost, speed, productivity, and quality of outputs and outcomes. The performance of IT in meeting organizational goals is so important that it is to be tied directly to funding decisions and reported up through agency channels for Congressional review.

1.1.1. Enterprise Information Technology Data Repository (EITDR) is the AF repository to identify all AF IT investments. All IT investments shall be identified within EITDR with the exception of items maintained within the Intelligence Community Registry or Nuclear Command, Control, and Computer Systems (NC3) Functional DAA. AFMC Special Access Programs/Special Access Required (SAP/SAR) IT investments are also exempt from registration in EITDR. Detailed AFMC guidance on what and how to answer EITDR questions will be maintained on the AFMC IT PfM Working Group (PfMWG) Collaboration Site.

1.2. IT Portfolios are comprised of a collection of IT Investments. Multiple ways exist to relate the IT Investments within AFMC. Therefore multiple IT portfolios exist and IT investments may belong to many IT portfolios depending on the perspective chosen.

1.2.1. IT investments are assigned to a Mission Area Lead based primarily on the DoD IT PfM Mission Areas and Domains, discussed in Section 1.5. However, architectural artifacts may better identify proper assignments and can be used in the assessment and assignment to the DoD Mission Areas and Domains. The primary architecture used for the Business Mission Area will be the DoD Business Enterprise Architecture (BEA) used by the Defense Business Systems governance structure. However, other architectures, such as the Federal Enterprise Architecture (FEA) Business Reference Model (BRM) and the DoD Architectural Framework (DoDAF), are used for all mission areas.

1.2.2. IT investments are assigned to an IT Sub-Portfolio Owner based on funding sources. Since AFMC is a support command and implements/sustains IT investments with funds from other AF commands/organizations, normally these supported IT investments shall be in the funding organization's portfolio. However, depending on traceability of these funds, these shall be organizationally assigned based on the Program Management Office's (PMO) organizational alignment.

1.3. The following four phases are associated with IT PfM activities (reference DoDD 8115.01, DoDI 8115.02, & AFI 33-141). As a basis for performing the four phases, the applicable architectural artifacts should be used to understand necessary capabilities. These IT PfM activities are applied to validate new IT investments for alignment to the IT portfolio, continuously monitor IT investments within the IT portfolio, identify IT investments for consideration to realign to another IT portfolio, and identify IT investments to remove/terminate. IT portfolios should be evaluated from both mission area and operational perspectives (e.g. Facility, Assets (Hardware/SW/Infrastructure), Application, Human Capital, Operations, and IT Services) in order to develop, collect, and present metrics to help with IT investment issues, IT compliance, and IT efficiency progress.

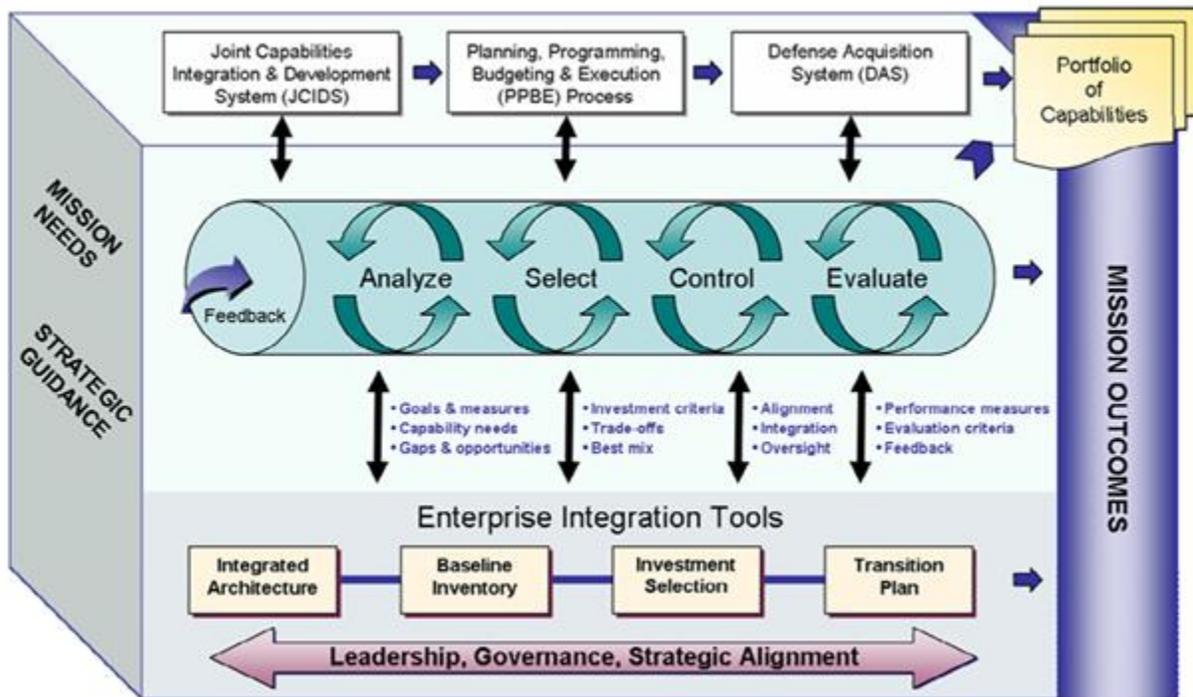
1.3.1. Analysis - Links IT portfolio objectives to DoD/Air Force Enterprise vision, mission, goals, objectives, and priorities; aligns to respective Core Function Master Plan(s); develops quantifiable outcome-based performance measures; identifies capability gaps, opportunities, and redundancies based on review of the architecture; identifies risks; and provides for continuous process improvement.

1.3.2. Selection - Identifies and selects the best mix of IT investments; strengthens and achieves capability goals and objectives for the IT portfolio in view of identified gaps, opportunities and redundancies derived from review of the architecture; ensures efficient and effective delivery of capabilities to the AFMC mission; maximizes return on investment to the AFMC Enterprise; demonstrates the impact of alternative IT investment strategies and funding levels.

1.3.3. Control - Ensures an IT portfolio is managed and monitored using established program management principles and quantifiable outcome-based performance measures; monitors and evaluates against IT portfolio performance measures to determine whether to recommend continuation, modification, or termination of individual investments within the IT portfolio.

1.3.4. Evaluation - Measures actual contributions of the IT portfolio and its individual investments against established outcome-based performance measures to determine that capability has improved or to support adjustments to the mix of IT portfolio investments, as necessary.

Figure 1. IT Portfolio Management Decision Support Interactions DoDI 8115.02.



1.4. IT PfM is used to identify all the IT investments (e.g., systems, initiatives, applications, tools, infrastructure, services, etc.), regardless of funding organization and appropriation needed to meet that operating configuration. IT portfolio reviews, with Core Function Lead Integrators, Headquarters AF (HAF) and Air Staff (SAF) functional organizations, ensure that the interrelated set of applications required by the Command are funded and implemented consistent with AF plans and programs.

1.5. The Enterprise IT portfolio is divided into four main Mission Area portfolios, identified as: Business Mission Area (BMA), Warfighting Mission Area (WMA), DoD portion of Intelligence Mission Area (DIMA) and Enterprise Information Environment Mission Area (EIEMA). Each of these is further broken out into component IT portfolios and capability areas. AFMC will have a Mission Area Lead that is charged with reviewing the IT investments within their mission area. Definitions are maintained at the following location ([https://cs.eis.afmc.af.mil/sites/cio/PfM/Mission/Mission Area and Sub Domain Definitions.doc](https://cs.eis.afmc.af.mil/sites/cio/PfM/Mission/Mission%20Area%20and%20Sub%20Domain%20Definitions.doc)). The following are currently defined Mission Area Domains and the Sub-Mission Area Domains:

1.5.1. Business Mission Area (BMA)

1.5.1.1. Weapon System Lifecycle Management (WSLM)

1.5.1.2. Material Supply and Service Management (MSSM)

1.5.1.3. Real Property & Installation Lifecycle Management (RPILM)

1.5.1.4. Human Resource Management (HRM)

1.5.1.5. Financial Management (FM)

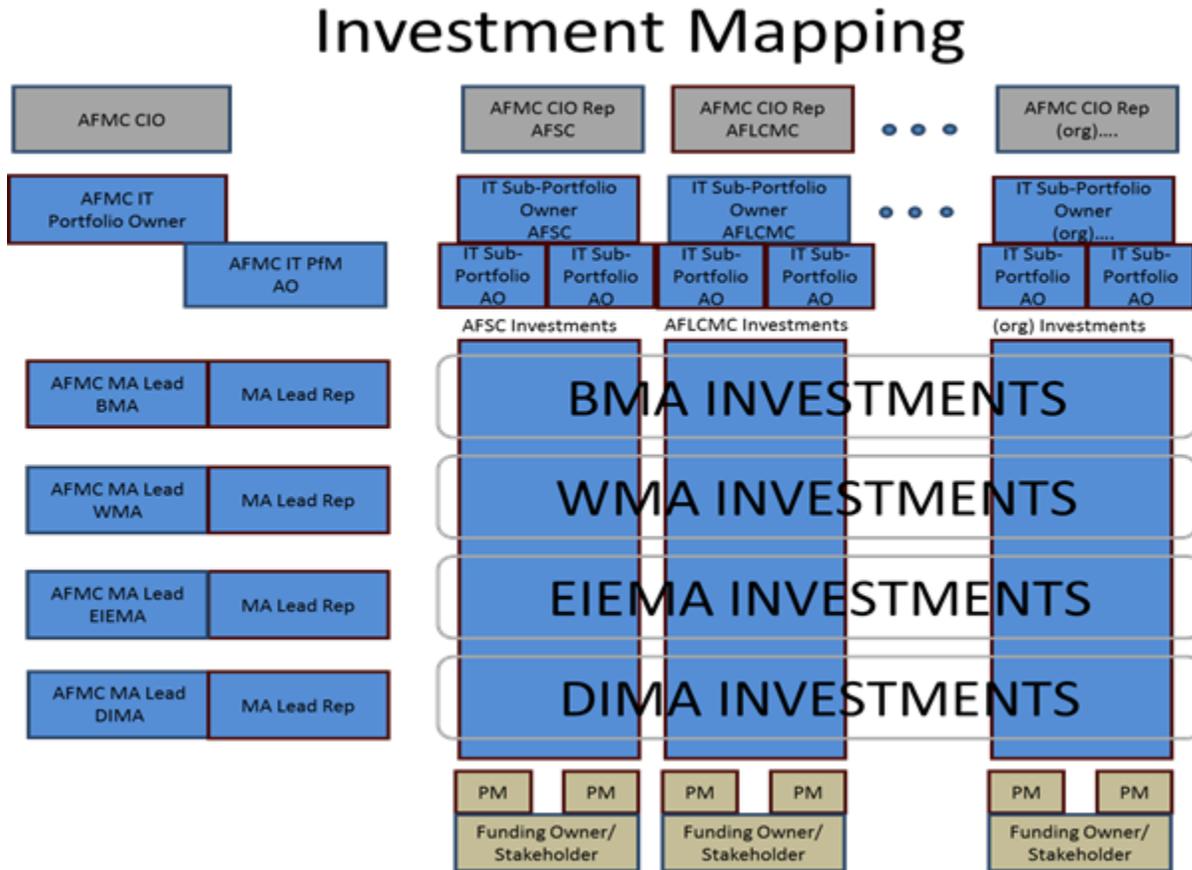
- 1.5.2. Warfighting Mission Area (WMA)
 - 1.5.2.1. Force Support (FS)
 - 1.5.2.2. Battlespace Awareness (BA)
 - 1.5.2.3. Force Application (FA)
 - 1.5.2.4. Logistics (L)
 - 1.5.2.5. Command and Control (C2)
 - 1.5.2.6. Net-Centric (NC)
 - 1.5.2.7. Protection (P)
 - 1.5.2.8. Building Partnerships (BP)
 - 1.5.2.9. Corporate Management and Support (CMS)
- 1.5.3. DoD portion of Intelligence Mission Area (DIMA)
 - 1.5.3.1. Defense Intelligence (DI)
 - 1.5.3.2. Enterprise Information Technology (EIT)
- 1.5.4. Enterprise Information Environment Mission Area (EIEMA)
 - 1.5.4.1. Communications Domain (COM)
 - 1.5.4.2. Information Assurance Domain (IA)
 - 1.5.4.3. Computing Infrastructure Domain (CMPI)
 - 1.5.4.4. Core Enterprise Services Domain (CES)

1.6. AFMC must also consider all types of Research, Development, Test, and Evaluation (RDT&E) IT investments associated with AFRL and the Test Centers. This includes the work done on networks internal to the Labs and the Test Centers (i.e. Standalone environments, Defense Research Network (DREN), commercial ISP) and on a limited basis the Air Force operational network environment. RDT&E IT investments are required to submit all of their technical reports associated with the project to the Defense Technical Information Center (DTIC). The Defense Department of Research & Engineering (DDR&E) Enterprise, the lead in the management of defense laboratories at the OSD level, will make the decisions on the RDT&E activities in coordination with the Air Force and Secretary of Defense. Scientific and Technical (S&T) reporting covers all areas of defense research, including biological and medical science, environmental pollution and control, and behavioral and social science. Therefore, managing the RDT&E IT investments using the processes referenced in DoDD 5134.3 and AFPD 61-1 take the place of the four IT PfM phases (Section 1.3). These IT investments will get assigned to the proper Mission Area per JCA guidance (reference CJSCI 8410.01A) and currently the WMA-CMS Mission Area addresses the RDT&E IT investments (see Attachment 2 for WMA-CMS breakout detail). However, other IT compliance reporting may still be required. The detailed guidance for IT compliance reporting is maintained at the AFMC IT PfM Collaboration Site.

2. Roles:

2.1. The following diagram contains a pictorial view of how the Mission Areas align with the roles discussed in 2.2 through 2.11.

Figure 2. IT Investment Mission Area Mapping to Roles.



2.2. AFMC CIO: Leads the command in establishing command-wide processes for IT PFM. The AFMC CIO empowers the Mission Area (MA) Leads (Section 2.4) and AFMC CIO Representatives (Section 2.6) to represent the IT portfolios on IT investment matters and allow him/her maximum latitude in working across organizational units to meet the requirements of federal law on IT investments. There currently is no delegation of official AF CIO responsibilities to MAJCOM CIOs. The AFMC CIO will provide IT vision, direction and corporate oversight of AFMC IT resources, needs and policy in support of AFMC’s strategic goals and objectives. For AFMC, the following are important CIO responsibilities expected to be carried out by the AFMC CIO:

2.2.1. Monitors the performance of IT programs of AFMC, evaluates the performance of those programs on the basis of the applicable performance measurements, and advises the AFMC Council regarding whether to continue, modify or terminate an IT program or project.

2.2.2. Annually, as part of the strategic planning and performance evaluation process, assess the IT requirements for facilitating the achievement of the performance goals established for the command information resources management.

2.2.3. Assesses the extent to which the IT positions and personnel at the executive level and Center levels of AFMC meet requirements. Develops strategies and specific plans for hiring, training, and professional development to rectify any deficiency in meeting requirements.

2.2.4. Provides advice, metrics, and other assistance to AFMC leadership (e.g. CC, CV, CA, AFMC Council, HQ AFMC 2-Letters, Center Commanders, etc.) to ensure that information technology is acquired and information resources are managed for AFMC in a manner that implements the policies and procedures of USC Title 10 and Title 40.

2.2.5. Establish an AFMC IT baseline and chart the course for a future Command-wide standards-based state.

2.3. AFMC IT Portfolio Owner: Shall have oversight responsibility for all IT investments within AFMC. To ensure IT resources are used efficiently within the command, need to validate the IT PfM four phases (described in Section 1.3) are implemented within mission area and organizational processes. As a cross-cutting role within AFMC, the AFMC IT Portfolio Owner will have representation on all AFMC Resource Management Panels to provide IT investment information and recommendations to the AFMC corporate board structure. Responsibility for reporting to senior leadership (e.g. CC, CV, CA) the health of the command IT portfolio. Shall be the final arbitrator in regard to disputes within the command between Mission Area Leads, IT Sub-Portfolio Owners, or between other roles/responsibilities in IT PfM matters. Annually certifies to the Air Force CIO, that the IT Portfolio information (budgetary and compliance data) provided is complete, accurate, and in accordance with current Air Force IT PfM direction (e.g., as provided in policy, Annual Planning and Programming Guidance, Program Objective Memorandum Preparation Instructions, etc.). Assigns the AFMC IT PfM Action Officer (AO) for implementation and guidance of the AFMC IT PfM processes to ensure all responsibilities are met. The AFMC IT Portfolio Owner determines the scope of IT investments within the AFMC IT Portfolio. AFMC IT Portfolio Owner assigns IT investments primarily by organization that contains the funding owner. However, it is not necessarily the case that all IT portfolio resources fall within the IT Sub-Portfolio Owner's organizational budget. The AFMC IT PfM Owner may assign an IT investment based on other factors (for example, AF Lead Program Management responsibility). AFMC/CC is the Core Function Lead Integrator (CFLI) for the Agile Combat Support (ACS) Service Core Function (SCF). Therefore, AFMC implements and sustains IT investments for other MAJCOMs; these IT investments are resourced with funds from outside AFMC, traceable to the ACS CFLI through capability alignment. The AFMC IT Portfolio Owner will work with HQ AFMC 2-Letters (e.g., A8/9, A2/5, etc.) to determine impacts and further processes needed from an IT PfM perspective on the ACS CFLI investments. The Collaboration Site maintained for the AFMC IT Portfolio Owner is located and shared on EIM for the AFMC IT PfM, IT Sub-Portfolio and CIO communities (<https://cs.eis.afmc.af.mil/sites/cio/PfM/default.aspx>).

2.4. AFMC MA Leads: This role is used to govern, from a functional perspective, the BMA, WMA, DIMA and EIEMA Mission Areas at the sub-domain level. MA Leads are functionally responsible for oversight of their Mission Area and for implementing the IT PfM four phases (analyze, select, control, and evaluate) mentioned in Section 1.3 to manage functional duplication for the IT investments being reported within their Mission Area. MA Leads will work closely with the AFMC IT Portfolio Owner to provide a complete accounting of all IT investments residing within a specific Mission Area to include the sub-categories that reside within those Mission Areas. MA Leads will include the AFMC IT Portfolio Owner in establishing and executing processes and procedures to meet all AF IT compliances, policies and procedures. MA Lead responsibilities are identified in Section 3 of this instruction. Assigns the MA Lead Representative responsible to support, from a functional perspective, the implementation of the duties assigned to the MA Lead, and provides recommendations to the appropriate officials for consideration in the Command's decision support system. In order to execute their respective missions, MA Leads are highly encouraged to establish individual MA governance structures to review IT requirements and approve those requirements specific to the MA sub-domain. These processes will then be identified to A3/6 for awareness. All cross-cutting (affecting external MA's) requirements will be reviewed/approved by the AFMC Group. If no internal MA governance structure exists, requirements will be reviewed and approved/disapproved when the AFMC Group is chaired by the CIO.

2.5. Funding Owner/Stakeholder: Organization that provides the funds to develop, modernize, enhance, or sustain a specific IT investment. The long line of accounting or official AF documents (e.g., Program Management Directives) used to fund activities for the IT investment helps identify the proper organization. The funding owner/stakeholder assigns the Program Manager (PM) or the Program Management Office (PMO), who then assigns the PM. The funding owner identifies the funding codes to the PM who then must identify the codes within IT PfM tools for compliance reporting. The funding owner/stakeholder works with the PM to establish, assess and refine operational needs, attributes, performance parameters, and constraints that flow from and influence user described capabilities. These user defined needs/capabilities need to align with guidance provided by MA Lead IT governance structures.

2.6. AFMC CIO Representatives (AFMC CIO Reps): Performs CIO functions respective to their Center or HQ AFMC 2-Letter. Ensure planning and execution for effective information resources management support of AFMC and higher headquarters IT requirements. Represents the organization on all IT investment matters. AFMC CIO Reps represent, gather and submit organizational IT and information resource requirements to the AFMC CIO. They work with their host Center IT staff to communicate and enforce AF and AFMC IT infrastructure policy. Likewise, the AFMC CIO Rep ensures the host base network and communications organizations are represented in the planning stages of IT/information resource acquisition to identify network standards for performance early in the process and ensure these requirements are met. There will be one CIO Rep assigned per Center, and one CIO Rep per HQ AFMC 2-Letter. The following are important responsibilities expected to be carried out by the AFMC CIO Rep:

2.6.1. Provide advice and other assistance to the AFMC CIO to ensure that information technology is acquired and information resources are managed for the entire command in

a manner that implements USC Title 10 and Title 40 and direction contained within applicable Federal, DoD and AF publications.

2.6.2. Develop, maintain and facilitate the implementation of a sound, secure and integrated information technology architecture.

2.6.3. CIO Reps are highly encouraged to establish individual organizational governance structures to review IT requirements and approve those requirements specific to the organizational portfolio. These processes will then be identified to A3/6 for awareness. All cross-cutting (affecting external organizations) requirements will be reviewed/approved by the AFMC Group. If no internal CIO Rep governance structure exists, requirements will be reviewed and approved/disapproved when the AFMC Group is chaired by the CIO.

2.6.4. Ensure that IT investments enter the Corporate Structure commensurate with the proper funding thresholds as described in paragraph 4.2.1 of this document.

2.6.5. Promote the effective and efficient design and operation of all major information resources management processes to include improvements to IT work processes of AFMC.

2.7. IT Sub-Portfolio Owner: Responsible for implementing the IT PfM four phases mentioned in Section 1.3 to manage the IT investments being reported within their IT portfolio. Leads, advises, and assists the AFMC IT Portfolio Owner in establishing and executing processes and procedures to meet all AF IT compliances, policies and procedures. Responsible for communicating AFMC guidance and direction to their IT program/project managers, financial program/project managers, and others responsible for IT PfM data collection and maintenance and partnering with them to collect and manage IT PfM data to support Air Force IT PfM and other processes. Responsible for all compliance reporting (e.g., Federal Information Security Management Act (FISMA), IT Budget, CCA, E-Authentication, Business Enterprise Architecture (BEA), Financial Improvement and Audit Readiness (FIAR), Enterprise Sequencing Plan, Enterprise Transition Plan, IPv6, National Defense Authorization Act (NDAA), Records Management, Section 508, Interoperability, Privacy, etc.) for IT investments assigned to their IT portfolio. IT Sub-Portfolio Owners will cover all IT investments as assigned by the AFMC IT Portfolio Owner. The IT Sub-Portfolio Owner assigns the IT Sub-Portfolio Action Officer(s) (AO) for their respective organization. Expectation is there is one IT Sub-Portfolio Owner assigned per Center and HQ AFMC 2-Letter level.

2.8. AFMC IT PfM Action Officer (AO): Implementation arm of AFMC IT Portfolio Owner. Supports AF data reviews and validation that are sent from HAF and SAF functional Subject Matter Experts (SMEs). To ensure IT resources are used efficiently within the command, need to validate the IT PfM four phases (described in Section 1.3) are implemented within mission area and organizational processes. Oversees and administers AFMC IT PfM data collection and submission. Provides supplemental procedures, definitions, policy and guidance as required within AFMC to clarify and improve IT PfM processes. EITDR administrators for IT investments in the AFMC IT portfolio. Maintains the AFMC IT PfM Collaboration Site that shall be used to preserve implementation details of this AFMCI. This role will have other responsibilities as defined further in AFMAN 33-408 when released.

2.9. IT Sub-Portfolio Action Officers (AOs): The implementation arm of the IT Sub-Portfolio Owners. Communicates guidance and works with AFMC IT PfM AO and Program Managers to effectively capture pertinent data to comply with IT Policy and laws. Working level at the Center/HQ 2-Letter supporting data reviews and validation, oversees and administers organizational IT PfM data collection and submission, and provides supplemental policy and guidance as required within their organization. EITDR administrators for IT investments in their IT portfolio. IT Sub-Portfolio AOs are the local approval authority for submitting any data updates and/or change requests to AFMC IT PfM AO to be ultimately approved by SAF/CIO A6. As necessary the IT Sub-Portfolio AOs will coordinate these changes with the AFMC IT PfM AO, AFMC Mission Area Leads, AFMC CIO Reps, and IT Sub-Portfolio Owners as applicable.

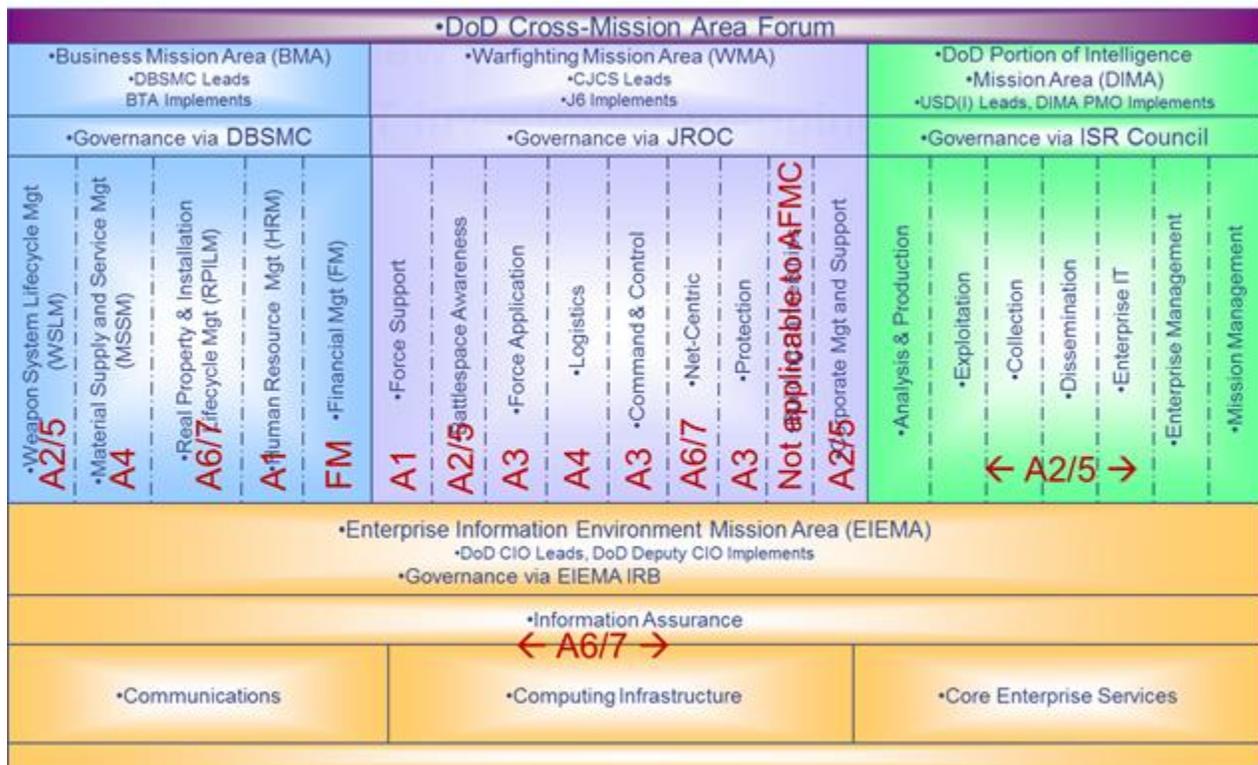
2.10. Mission Area Lead Representatives: Assigned by the Mission Area Lead for the implementation of the Mission Area Lead duties. Primary responsibility is to implement the IT PfM four phases (described in Section 1.3) to help ensure IT resources are used efficiently within the command.

2.11. Program Manager (PM): This is the person responsible for sustainment or implementation of a specific IT investment. The PM reviews and corrects all budgetary and programmatic detail, maintains all supporting documentation and is responsible for all information entered into IT PfM tools (e.g., EITDR, ACART, ABE, etc.). PM's are required to identify themselves in the Points of Contact field within EITDR, and are to periodically review EITDR data for accuracy and completeness. From an IT PfM perspective this can be assigned formally through major IT efforts that meet AF guidance thresholds or informally through local IT efforts. The PM is responsible for the cost, schedule and technical performance of the IT investment to which they are assigned per DoDI 5000.02 and AFI 63-101. The PM is ultimately responsible for all compliance requirements.

3. Responsibilities:

3.1. The following diagram contains a pictorial view of the responsibilities of the MA Leads as assigned in 3.2 through 3.9.

Figure 3. IT Portfolio Structure AFMC Assignment.



3.2. HQ AFMC/A3/6:

3.2.1. Assigned as the AFMC CIO.

3.2.2. Assigned as the AFMC IT Portfolio Owner. Oversee the entire IT PfM processes and governance policies/procedures for AFMC.

3.2.3. Assigned the Mission Area Lead for the AFMC EIEMA investments. Delegate others to manage the EIEMA investments when necessary, but must maintain central authority as the Mission Area Lead.

3.2.4. Assigned the Mission Area Lead for the AFMC BMA-RPILM investments. Delegate others to manage the BMA-RPILM investments when necessary, but must maintain central authority as the Mission Area Lead.

3.2.5. Assigned the Mission Area Lead for the AFMC WMA-NC investments. Delegate others to manage the WMA-NC investments when necessary, but must maintain central authority as the Mission Area Lead.

3.2.6. Supports HQ AFMC/A4 for the AFMC WMA-L investments that pertain to Security Forces and Civil Engineering functions.

3.2.7. HQ AFMC/A6I:

3.2.7.1. Assigned as the AFMC IT PfM Action Officer (AO). Delegate within A6I to manage the AFMC IT investments when necessary.

3.2.7.2. Assigned as the Mission Area Lead for WMA-NC, EIEMA and BMA-RPILM. Delegate within A6I to manage the AFMC IT investments when necessary.

3.2.7.3. Develops, collects, and presents metrics to help AFMC with IT investment issues, IT compliance, and IT efficiency progress.

3.3. HQ AFMC/A1:

3.3.1. Assigned the Mission Area Lead for the AFMC BMA-HRM investments. Delegate others to manage the BMA-HRM investments when necessary, but must maintain central authority as the Mission Area Lead.

3.3.2. Assigned the Mission Area Lead for the AFMC WMA-FS investments. Delegate others to manage the WMA-FS investments when necessary, but must maintain central authority as the Mission Area Lead.

3.3.3. Involve/support other HQ AFMC 2-Letters as necessary based on functional expertise.

3.4. HQ AFMC/A2/5:

3.4.1. Assigned the Mission Area Lead for the AFMC BMA-WSLM investments. Delegate others to manage the BMA-WSLM investments when necessary, but must maintain central authority as the Mission Area Lead. HQ AFMC/PK will maintain the lead for those IT investments that pertain to Contracting functions.

3.4.2. Assigned the Mission Area Lead for the AFMC DIMA investments. Delegate others to manage the DIMA investments when necessary, but must maintain central authority as the Mission Area Lead.

3.4.3. Assigned the Mission Area Lead for the AFMC WMA-BA investments. Delegate others to manage the WMA-BA investments when necessary, but must maintain central authority as the Mission Area Lead.

3.4.4. Assigned the Mission Area Lead for the AFMC WMA-CMS investments. Delegate others to manage the WMA-CMS investments when necessary, but must maintain central authority as the Mission Area Lead. HQ AFMC/A8/9 will maintain the lead for those IT investments that pertain to strategy and programming. HQ AFMC/A3 will maintain the lead for those IT investments that pertain to DT&E.

3.4.5. Provides expertise to the AFMC CIO and the AFMC CIO Reps in validating SAP/SAR IT investments.

3.4.6. Involve/support other HQ AFMC 2-Letters as necessary based on functional expertise.

3.5. HQ AFMC/A3:

3.5.1. Assigned the Mission Area Lead for the AFMC WMA-C2 investments. Delegate others to manage the WMA-C2 investments when necessary, but must maintain central authority as the Mission Area Lead.

3.5.2. Assigned the Mission Area Lead for the AFMC WMA-FA investments. Delegate others to manage the WMA-FA investments when necessary, but must maintain central authority as the Mission Area Lead.

3.5.3. Assigned the Mission Area Lead for the AFMC WMA-P investments. Delegate others to manage the WMA-P investments when necessary, but must maintain central authority as the Mission Area Lead.

3.5.4. Involve/support other HQ AFMC 2-Letters as necessary based on functional expertise.

3.6. HQ AFMC/A4:

3.6.1. Assigned the Mission Area Lead for the AFMC BMA-MSSM investments. Delegate others to manage the BMA-MSSM investments when necessary, but must maintain central authority as the Mission Area Lead.

3.6.2. Assigned the Mission Area Lead for the AFMC WMA-L investments. Delegate others to manage the WMA-L investments when necessary, but must maintain central authority as the Mission Area Lead.

3.6.3. Involve/support other HQ AFMC 2-Letters as necessary based on functional expertise.

3.7. HQ AFMC/A8/9:

3.7.1. Assigned the Mission Area Lead for the AFMC WMA-CMS investments that pertain to planning, programming, and strategizing.

3.7.2. Involve/support other HQ AFMC 2-Letters as necessary based on functional expertise.

3.8. HQ AFMC/FM:

3.8.1. Assigned the Mission Area Lead for the AFMC BMA-FM investments. Delegate others to manage the BMA-FM investments when necessary, but must maintain central authority as the Mission Area Lead.

3.8.2. Involve/support other HQ AFMC 2-Letters as necessary based on functional expertise.

3.8.3. Provides FIAR advice and assistance to CIO, BMA Leads, and related IT personnel.

3.9. HQ AFMC/PK:

3.9.1. Assigned the Mission Area Lead for the AFMC BMA-WSLM investments that pertain to Contracting functions.

3.9.2. Involve/support other HQ AFMC 2-Letters as necessary based on functional expertise.

3.10. All HQ AFMC 2-Letters:

3.10.1. Provide functional expertise to the assignees of any role identified in Section 2 as necessary.

3.10.2. Designate the Mission Area Lead Representative, AFMC CIO Rep and IT Sub-Portfolio Owner for the organization to AFMC IT PFM AO mailbox (AFMC.A6.PfM@wpafb.af.mil).

3.10.3. Implement the IT PFM phases (described in Section 1.3) to ensure controls are in place for approval of new IT investments within functional area of expertise and IT resources are used efficiently within the command.

3.10.4. Ensure the appropriate PK Contracting Office is involved in the acquisition of anything IT to validate the proper NDAA procedures have taken place prior to the expenditure of funds.

3.11. All Center Commanders:

3.11.1. Provide functional expertise to the assignees of any role identified in Section 2 as necessary.

3.11.2. Centralize oversight and management of IT development, modernization and sustainment efforts within their areas of responsibility.

3.11.3. Consolidate all IT resources that implement and/or sustain any IT investments into an organizational structure that allows for consolidation and efficiency of these IT resources.

3.11.4. Implement the IT PFM phases (described in Section 1.3) to ensure controls are in place for approval of new IT investments within functional area of expertise and IT resources are used efficiently within the Center.

3.11.5. Designate the AFMC CIO Rep and IT Sub-Portfolio Owner for the organization to AFMC IT PFM AO mailbox (AFMC.A6.PFM@wpafb.af.mil).

3.11.6. Ensure the appropriate PK Contracting Office is involved in the acquisition of anything IT to validate the proper NDAA procedures have taken place prior to the expenditure of funds.

3.12. AFMC Communication Units:

3.12.1. Ensure no IT investment is connected to the AF network without being registered or covered by a registered entry in appropriate IT PFM tools.

3.12.2. Approve all EIEMA IT investments within a base to ensure they meet DoD, AF, and AFMC CIO guidance and plans before installation on the AF Network.

3.12.3. Provides computer center hosting (other than DISA) and network/desktop capability for Center and Laboratory applications as well as normal business office IT operations across the installation.

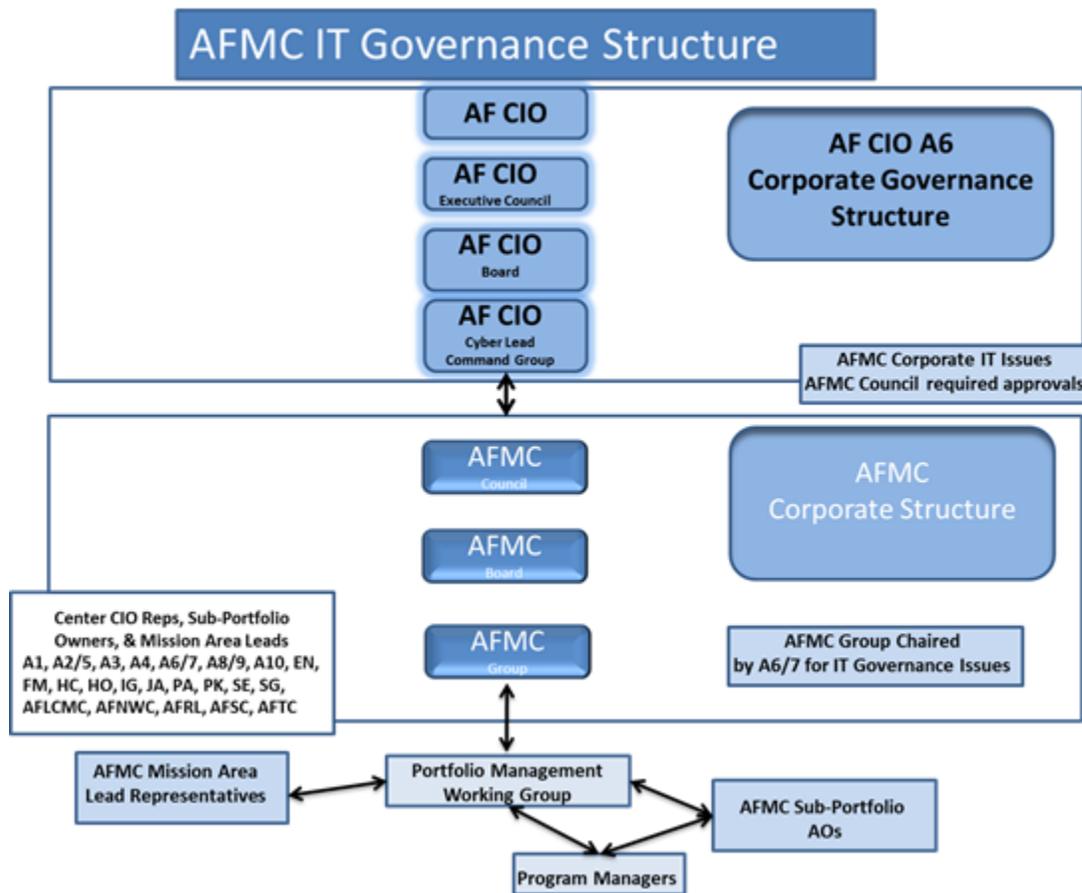
3.12.4. Establish processes to ensure all IT Requirements are vetted in accordance with AFMC IT PFM processes and appropriate Mission Areas.

4. AFMC IT PFM Processes and Governance Structure:

4.1. Detailed AFMC IT PFM Standard Processes to abide by are maintained at the following location within the IT PFM Collaboration Site (<https://cs.eis.afmc.af.mil/sites/cio/PfM/Processes/Forms/AllItems.aspx>).

4.2. AFMC IT Governance Structure. The following diagram depicts the high-level organization of the AFMC IT Governance structure and the relationship to other forums.

Figure 4. AFMC IT Governance Structure.



4.2.1. AFMC Corporate Structure: The primary objective of the corporate board process, as outlined in AFMCI 90-601, is to provide the AFMC Commander and Staff with the capability to review Command-wide issues from a corporate perspective and maximize the effectiveness of AFMC's decision-making. The corporate structure is comprised of the AFMC Group, AFMC Board, and AFMC Council to vet planned initiatives/issues/plans for executive decisions. The Corporate Structure ensures the supporting and dissenting opinions for all major decisions are captured to enable senior Command leadership to make informed decisions. The AFMC Group, AFMC Board and AFMC Council are the forums to support the AFMC CIO in his/her support of the AFMC Corporate Structure and ultimately the AFMC Commander. HQ AFMC/A3/6 will use the AFMC Council as the forum for its most critical AFMC CIO issues. These issues will first be vetted through the AFMC Group and AFMC Board. HQ 2-Ltr Functional offices and Center Commander's will ensure that all IT requirements are vetted through, and approved by, the corporate process prior to the expenditure of any funds against the requirement. All IT requirements will enter the corporate process at the AFMC Group level for requirement justification and evaluation.

4.2.1.1. HQ AFMC/A3/6 will utilize the AFMC Board to allow cross-functional review and evaluation of AFMC CIO issues. Some issues to be vetted involve OSD approvals for IT investment certifications and IT metrics for FISMA compliance.

Also, IT efficiencies progress would be vetted on how AFMC is spending money more effectively. The strength of the AFMC Board lies in its broad representative span that allows the reviewing of decision and thorough vetting of issues from the AFMC Group before elevating the most critical issues to the AFMC Council. HQ AFMC/A3/6 will chair the AFMC Group for topics affecting AFMC IT investments for improving and implementing information technology practices related to the design, acquisition, development, modernization, use, operation, sharing, and performance of AFMC information resources. The AFMC Group when chaired by the AFMC CIO will be made up of AFMC CIO Representatives, IT Sub-Portfolio Owners and Mission Area Leads. Other HQ AFMC 2-Letter representative will be added as necessary based on functional expertise needed. HQ AFMC/A3/6 will forward unresolved issues to the AFMC Board for resolution.

4.2.1.2. The following has been established for the purpose of IT investments review and funding approval when the AFMC Group is chaired by the AFMC CIO: Review/approve ALL cross-cutting (affecting multiple MAs or organizations) IT investments (including those approved within internal governance processes); and recommend IT investments with higher thresholds to the AFMC Board for review/approval. If no internal IT requirements approval process exists (discussed in Sections 2.4 and 2.6), then all IT requirements/investments will be reviewed/approved by the AFMC Group. All IT requirements that meet the DBS NDAA threshold for OSD certification are considered cross-cutting.

4.2.2. AFMC IT PFMWG: AFMC IT PFM AO chairs an IT PFMWG comprised of IT Sub-Portfolio AOs and MA Lead representatives. The AFMC IT PFM AO provides the latest issues, passes information from AF meetings, tracks compliance status, monitors application of the IT PFM phases by MA Leads and IT Sub-Portfolio Owners. AFMC IT PFMWG ensures required IT compliance reporting activities are met for AFMC assigned IT investments and works closely with their customers to capture the required information for AFMC IT portfolio investor maps, compliance forms, scorecards, and AFMC IT PFM dashboard criteria. The AFMC IT PFMWG performs corporate oversight of assigned IT portfolios and ensures the assigned investments within EITDR are correct. The AFMC IT PFMWG Collaboration Site (<https://cs.eis.afmc.af.mil/sites/cio/PfM/default.aspx>) and event calendar provide compliance tracking and supporting information for the group. This forum helps initiate recommendations from IT PFM activities into the AFMC CIO and AFMC IT Corporate Structure.

TERRY G. EDWARDS, P.E., SES
Director of Communications, Installations and
Mission Support

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

- Title 10 USC § 2222, *Defense Business systems: Architecture, Accountability, and Modernization*
- Title 10 USC § 2223, *Information Technology: Additional Responsibilities of Chief Information Officers*
- Title 10 USC § 2223a, *Information Technology Acquisition Planning and Oversight Requirements*
- Title 40 USC Subtitle III, *Information Technology Management (Clinger-Cohen Act of 1996 (CCA))*
- Title 44 USC, **Chapter 35**, *Coordination of Federal Information Policy*
- Executive Order 13011, *Federal Information Technology*, 16 July 1996
- DoD Financial Management Regulation (FMR) 7000.14-R Volume 2B, July 2013
- DoDD 8115.01, *Information Technology Portfolio Management*, 10 October 2005
- DoDD 5134.3, *Director of Defense Research and Engineering (DDR&E)*, 03 November 2003
- DoDI 5000.02, *Operation of the Defense Acquisition System*, 8 December 2008
- DoDI 8115.02, *Information Technology Portfolio Management Implementation*, 30 October 2006
- OMB Circular A-11, *Preparation, Submission and Execution of the Budget*, July 2013
- OMB Circular A-130, *Management of Federal Information Resources*, 28 November 2000
- JROCM 103-14, *2014 Refinement of the Joint Capability Areas*, 01 October 2014
- AFPD 17-1, *Information Dominance Governance and Management*, 12 April 2016
- AFPD 61-1, *Management of Science and Technology*, 18 August 2011
- AFI 33-141, *Air Force Information Technology Portfolio Management and IT Investment Review*, 23 December 2008
- AFI 33-150, *Management of Cyberspace Support Activities*, 21 August 2013
- AFI 63-101, *Integrated Life Cycle Management*, 07 March 2013
- AFMAN 33-363, *Management of Records*, 01 March 2008
- AFMCI 90-601, *AFMC Corporate Structure*, 11 March 2014
- Adopted Forms***
- AF Form 847, *Recommendation for Change of Publication*

Terms

Clinger—Cohen Act (CCA) - Enacted in 1996, the act modified the approach the US Government takes for the acquisition, use and disposal of IT. It elevated oversight responsibility to the Director of the Office of Management and Budget (OMB) and, among other requirements, established OMB responsibility to exercise capital planning control; develop a process for analyzing, tracking, and evaluating the risks and results of all major capital investments in information systems; coordinate the development and review of policy associated with Federal information technology acquisition. CCA defines what “IT” is and created the departmental Chief Information Officer (CIO) positions. It directs executive agencies (e.g., DoD and AF) to design and implement a process for maximizing the value and assessing and managing the risks of information technology acquisitions; to utilize performance- and results-based management practices, and to prepare an annual report to the Congress concerning progress in achieving such goals. (Subtitle III of Title 40 USC).

Enterprise Information Technology Data Repository (EITDR)—The AF system of record for IT Compliance management data. The AF IT processes and mandates supported by EITDR include AF IT initiative and systems Registration, AF IT Budget and Capital Investment Reporting (CIR), AF Federal Information Security Management Act (FISMA) compliance, Clinger-Cohen Act compliance, AF National Defense Authorization Act (NDAA) certification, AF IT Lean acquisition, AF Privacy Impact Assessment (PIA), E-Government Act of 2002 (Records Management), Section 508 compliance and others. (AFI 33-141).

Information Resources—Information and related resources, such as personnel, equipment, funds and Information Technology (IT). (DoDI 8115.02).

Information Resources Management (IRM)—The process of managing information resources to accomplish agency missions and to improve agency performance, including through the reduction of information collect burdens on the public. (Section 3502, Subchapter I of Title 44, Chapter 35).

Information System (IS)—A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Section 3502, Subchapter I of Title 44, Chapter 35).

Information Technology (IT)— The term “information technology”- (A) with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, 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 (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product; (B) includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but (C) does not include any equipment acquired by a federal contractor incidental to a federal contract. (Section 11101, Subtitle III of Title 40 USC, chapter 111).

IT Investment—The development and sustainment resources needed in support of IT. These resources include, but are not limited to: research, development, test, and evaluation appropriations; procurement appropriations; military personnel appropriations; operations and maintenance appropriations; and Defense Working Capital Fund. Investment includes all IT spending. (DoDD 8115.01).

IT Portfolio— The collection of capabilities, resources and related investments that are required to accomplish a mission-related or administrative outcome. A portfolio includes outcome performance measures (mission, functional or administrative measures) and an expected return on investment. “Resources” include people, money, facilities, weapons, IT, other equipment, logistics support, services and information. (AFI 33-141).

IT Portfolio Management Activities—Management activities for the portfolio include strategic planning, capital planning, governance, process improvements, performance metrics/measures, requirements management, IT Investment go/no-go decisions, acquisition/development and operations. (AFI 33-141).

Attachment 2**BREAKOUT FROM JCA OF WMA-CMS****A2.1. Corporate Management and Support**

- A2.1.1. Advisory and Compliance
 - A2.1.1.1. Advice and External Matters
 - A2.1.1.1.1. Legal Matters
 - A2.1.1.1.2. Legislative Matters
 - A2.1.1.2. Audit, Inspection and Investigation
 - A2.1.1.2.1. Audits
 - A2.1.1.2.2. Inspections
 - A2.1.1.2.3. Investigations
 - A2.1.1.3. Operational Test and Evaluation
- A2.1.2. Strategy and Assessment
 - A2.1.2.1. Strategy Development
 - A2.1.2.2. Capabilities Development
 - A2.1.2.3. Enterprise-Wide Assessment
 - A2.1.2.4. Studies and Analyses
 - A2.1.2.5. Enterprise Architecture
- A2.1.3. Information Management
- A2.1.4. Acquisition & Technology
 - A2.1.4.1. Research
 - A2.1.4.1.1. Basic
 - A2.1.4.1.2. Applied
 - A2.1.4.2. Advanced Technology
 - A2.1.4.2.1. Capability Experimentation
 - A2.1.4.2.2. Capability Demonstration
 - A2.1.4.3. Developmental Engineering
 - A2.1.4.3.1. Systems Engineering & Manufacturing
 - A2.1.4.3.2. Developmental Testing
 - A2.1.4.4. Acquisition
 - A2.1.4.4.1. Program Initiation
 - A2.1.4.4.2. Contracting

- A2.1.4.4.3. Portfolio System Acquisition
- A2.1.4.4.4. Production & Lifecycle Acquisition
- A2.1.4.4.5. Capability Termination & Disposal
- A2.1.5. Program, Budget and Finance
 - A2.1.5.1. Program / Budget and Performance
 - A2.1.5.2. Accounting and Finance