BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 17-110

23 MAY 2018

Cyberspace Operations

INFORMATION TECHNOLOGY PORTFOLIO MANAGEMENT AND CAPITAL PLANNING AND INVESTMENT CONTROL

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/CIO A6XM

Certified by: SAF/CIO A6X
(Mr. Arthur "A.G." Hatcher)

Supersedes: AFI33-141, 23 December 2008

Pages: 33

This instruction implements Air Force Policy Directive (AFPD) 17-1, *Information Dominance Governance and Management*, Headquarters Air Force Mission Directive (HAF MD) 1-26, *Chief, Information Dominance and Chief Information Officer*, Department of Defense (DoD) Directive 8115.01, *Information Technology Portfolio Management*, DoD Instruction 8115.02, *Information Technology Portfolio Management Implementation*. It assigns responsibilities and provides guidance for Information Technology Portfolio Management and conducting Capital Planning and Investment Control for Information Technology investments throughout the Air Force. It applies to individuals at all levels who manage Information Technology resources including the Air Force Reserve and Air National Guard except where noted otherwise. This publication may be supplemented at any level, but all supplements must be routed to the Office of Primary Responsibility (OPR) listed above for coordination prior to certification and approval. Refer recommended changes and questions about this publication to the OPR listed above using the Air Force Form 847, *Recommendation for Change of Publication*; route Air Force Form 847 from the field through the appropriate 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 Air Force Instruction 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 requested commander for non-tiered compliance items. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of

in accordance with the Air Force Records Disposition Schedule in the Air Force Records Information Management System.

SUMMARY OF CHANGES

This is a total revision of Air Force Instruction 17-110, *Air Force Information Technology Portfolio Management and IT Investment Review,* dated 23 December 2008. This document has been substantially revised and formalizes the Information Technology Portfolio Management process and identifies the processes in which Capital Planning and Investment Control elements are accomplished. A complete revision to the guidance and responsibilities for performing Information Technology Portfolio Management throughout the Department is provided herein. The guidance prescribed in this document is consistent with the statutory and regulatory requirements, executive guidance and best practices in applicable policies listed above. The Air Force shall comply with the Portfolio Management/Capital Planning and Investment Control and Information Technology management guidelines listed herein.

Chapter 1

INFORMATION TECHNOLOGY PORTFOLIO MANAGEMENT AND CAPITAL PLANNING AND INVESTMENT CONTROL

1.1. Purpose and Overview of Information Technology Portfolio Management and Capital Planning and Investment Control.

1.1.1. In accordance with DoD Directive 8115.01, the Air Force uses Portfolio Management to control its Information Technology investments using the Mission Area structure as the common framework and lexicon for the organization of Information Technology portfolios. Information Technology Portfolio Management has three main goals: maximize the value of the portfolio against the objectives of DoD; balance the portfolio against resource constraints; link the portfolio to strategy. An essential element of Portfolio Management is Capital Planning and Investment Control of Information Technology investments. Through Portfolio Management and proper Capital Planning and Investment Control, Information Technology investments deliver the most capability to Airmen to conduct operations across all Mission Areas.

1.1.2. This Instruction implements and establishes Air Force-wide guidance, roles and responsibilities for the Air Force's Information Technology Portfolio Management and Capital Planning and Investment Control as follows:

1.1.2.1. Further defines Portfolio Management and Capital Planning and Investment Control and how these processes are accomplished through the DoD principal decision support and the Air Force corporate structure processes.

1.1.2.2. Assigns responsibilities for the management of Air Force Information Technology investments, including National Security Systems (in accordance with statutory requirements) and its associated resources as portfolios within the Air Force Enterprise that focus on improving Air Force and DoD capabilities and mission outcomes.

1.1.2.3. Provides fundamental concepts for managing a portfolio of Information Technology resources and defines processes for complying with external and internal statutory and regulatory requirements.

1.1.2.4. Establishes a management framework within the Air Force to develop and manage Information Technology portfolios by Mission Area at all levels in which the Air Force develops, manages, or funds Information Technology investments.

1.1.2.5. Provides guidance on how the content of these portfolios will be documented to support the Air Force Information Technology Portfolio Management and decision-making processes in the Office of Information Dominance and Chief Information Officer in concert with DoD decision support and Air Force corporate structure processes.

1.1.2.6. Defines and clarifies requirements for identifying and registering Information Technology resources comprising an initiative (systems, programs, projects, organizations, and families of systems) within the Air Force Information Technology Investment Portfolio Suite (referred to as ITIPS).

1.2. Portfolio Management and Capital Planning and Investment Control Concepts.

1.2.1. Information Technology investments shall be managed as portfolios to ensure these investments support the Air Force's vision, mission and goals; ensure efficient and effective delivery of capabilities to the warfighter; and maximize return on investment to the enterprise. All Information Technology investments must be approved through the appropriate DoD decision support and Air Force corporate structure process. Once approved, all Information Technology investments will be registered in ITIPS by the program or project manager with assistance provided by the Portfolio Manager (or an equivalent system for Special Access Programs). SAF/CIO A6 staff will initiate registration in DoD's Information Technology Portfolio Repository (DITPR) system and upload to the Defense Information Technology Investment Portal (DITIP) to obtain a Select & Native Programming Data Input System for Information Technology (SNaP-IT) Unique Investment Identifier (for new investments only).

1.2.2. Information Technology Portfolios shall be grouped and integrated at the DoD Mission Area and Functional levels. Specifically, the portfolios are defined in their respective Mission Area - Warfighting Mission Area, Business Mission Area, Information Environment Mission Area and the Defense Intelligence Mission Area. Functional portfolios are defined by their Functional area such as logistics, personnel and training. Mission Area and Functional portfolios may be divided into subportfolios (e.g., domains) that represent common collections of related, or highly dependent, system capabilities and services. These portfolios/subportfolios are managed by the appropriate Portfolio Owners. Further information on the Mission Areas and their respective portfolios/subportfolios are described in section 1.4 Portfolio Governance.

1.2.3. Effective and efficient management of Information Technology Investment portfolios is a result of the complementary application of Capital Planning and Investment Control principles within the processes of Joint Capabilities Integration and Development System (if applicable investment value is met) & Defense Acquisition System, or Business Capability Acquisition Cycle and Planning, Programming, Budgeting and Execution processes as outlined in DoD Instruction 8115.02. Capital Planning and Investment Control enables the selection, control and evaluation for every Information Technology investment and renders a recommendation to reviewing boards for inclusion in the Air Force Organizational Execution Plans and/or Core Function Support Plans (note: the analysis activities of capital planning and investment control listed in DoD Instruction 8115.02 are covered in the selection activities of Attachment 6). Portfolio Owners and Managers (this term is hereafter used as all-inclusive of Mission Area portfolios, sub-portfolios and Functional portfolios) use the information gleaned from Capital Planning and Investment Control evaluations to better inform decisions on Information Technology systems and assess capability gaps within their portfolio. The execution of this process will encompass all DoD Mission Areas.

1.3. Portfolio Management and Capital Planning and Investment Control Objectives.

1.3.1. The overarching objective of Portfolio Management is to ensure Information Technology investment decisions take into account integration, coordination and synchronization of capability requirements to Information Technology investments. Additionally, Portfolio Management ensures that proper evaluation of the capability demand (both warfighting and non-warfighting) is balanced against resource constraints, risks are

identified and assessed and possible trade-offs are identified to Air Force decision makers (SAF/CIO A6, Headquarters Air Force Functionals, Portfolio Owners). Other Portfolio Management objectives are as follows:

1.3.1.1. Demonstrate and document clear alignment of the Information Technology Portfolio to Air Force's mission and business objectives and with the strategic and tactical goals specified in the Information Dominance Flight Plan and the Air Force Strategic Master Plan.

1.3.1.2. Ensure sufficient and appropriate business planning and justification in the selection and control of Air Force Information Technology investments.

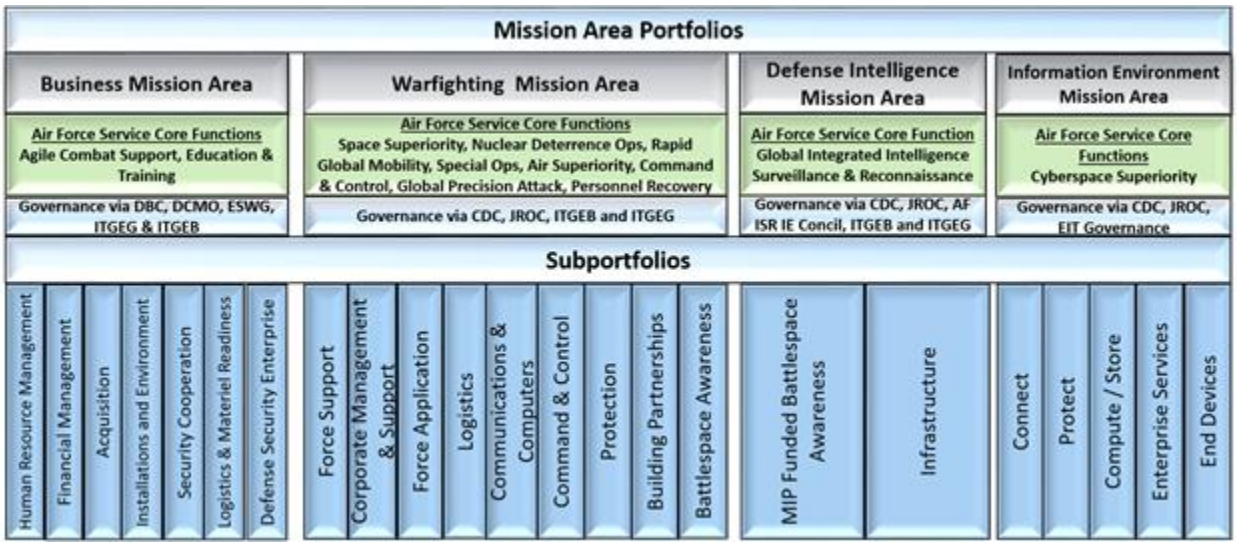
1.3.2. Capital Planning and Investment Control, as a whole, integrates strategic planning, Enterprise Architecture, cybersecurity, budgeting, portfolio management, risk management and acquisition management of Information Technology investments. These factors are evaluated throughout the life cycle of an investment through selection, control and evaluation (see Attachment 1 for definitions). Attachment 6 lists recommended questions during selection, control and evaluation that assist in ensuring a new Information Technology investment is tied to strategic guidance. These questions should be addressed by the Program Manager and/or project sponsor and reviewed by the Portfolio Manager, Portfolio Owners and by the appropriate interested SAF/CIO A6 directorates through the existing DoD decision support and Air Force corporate structure processes, reviews and documents.

1.3.3. The funding of investments within the portfolios is the result of the complementary application of Capital Planning and Investment Control principles within the Joint Capabilities Integration and Development System (requirements) and Defense Acquisition System (acquisition), or Business Capability Acquisition Cycle (requirements and acquisition for Defense Business Systems) and Planning, Programming, Budgeting and Execution (resourcing) processes as discussed in the sections that follow.

1.4. Portfolio Governance.

1.4.1. Portfolios of Information Technology investments must be managed using Capital Planning and Investment Control and will utilize, to the maximum extent possible, the DoD governance structure and key processes to address Mission Areas and their aligned Functional capability areas (see Figure 1.1). The primary DoD decision support processes are the processes of the Joint Capabilities Integration and Development System, Defense Acquisition System, Business Capability Acquisition Cycle and Planning, Programming, Budgeting and Execution. Figure 1.1 is a representation of the Mission Areas, the Air Force service core functions, DoD and Air Force governance and main subportfolios.

Figure 1.1. DoD Mission Areas, Service Core Functions, Governance and Subportfolios.



1.4.2. All Information Technology investments will be assessed annually using the Information Technology investment selection, control and evaluation reviews, depending on where in the life cycle an Information Technology investment is through DoD decision support processes and the governance structures described in this instruction.

1.4.3. All Information Technology investments must be aligned to Mission Areas and organized by the approved Mission Area guidance criteria. Upon initial registration in ITIPS (or an equivalent system for Special Access Programs), Portfolio and/or Program Managers will select a Mission Area (see Attachments 2-5 as guidance on selecting a Mission Area) based on their knowledge of proper alignment of the Information Technology investment. SAF/CIO A6 staff, will review input and make a recommendation on the Mission Area and validate it with the Mission Area Portfolio Owner as part of the registration review process. Further information on ITIPS can be found in section 1.6.

1.4.4. All Mission Areas and aligned Functional capability areas will be managed and governed using an integrated approach based on the Air Force Enterprise Architecture capability goals and objectives, principles, rules, activities, processes, services, standards and performance measures (reference Air Force Instruction 17-140, *Air Force Architecting*).

1.4.5. Special Access Program Information Systems must comply with this instruction unless they also handle Sensitive Compartmented Information material. More restrictive Intelligence and Special Access Program policies and directives take precedence over this publication. The latest version of all publications (e.g., Federal, Joint, DoD, Air Force) referenced within this publication must be used.

1.5. Portfolio Management/Capital Planning and Investment Control Alignment with Corporate Structure Processes.

1.5.1. The DoD decision support processes (reference paragraph 1.4.1) are conducted at the service level by the Air Force corporate structure (Air Force Requirements Oversight Board, Air Force Council and the Air Force Review Board). The Air Force's Portfolio Management and Capital Planning and Investment Control must be aligned to DoD decision support processes, Air Force corporate structure processes and Air Force Enterprise Architecture to

the maximum extent possible. By integrating Portfolio Management/Capital Planning and Investment Control into these existing processes, the Air Force is better able to make informed decisions on Information Technology investments as they are acquired, maintained and decommissioned.

1.5.2. With respect to assignment of a specific Information Technology investment to an organizational portfolio, the organization that plans and programs resources supporting the investment through the Planning, Programming, Budgeting and Execution cycle is responsible for performing Portfolio Management and Capital Planning and Investment Control activities throughout the lifecycle of the investment. Where multiple organizations plan and program resources to support a single Information Technology investment, the organization identified as lead command or that provides the largest percentage of funds, in the absence of a lead command, is responsible for performing Portfolio Management and Capital Planning and Investment Control activities for that investment.

1.6. Information Technology Investment Portfolio Suite (ITIPS).

1.6.1. The Information Technology Investment Portfolio Suite, referred to as ITIPS, is the Air Force's enterprise authoritative source for Information Technology portfolio management and is used to report both Information Technology compliance and budget. For Information Technology compliance, these functions include processes for Information Technology Registration, Privacy Act, Federal Information Security Modernization Act, Clinger-Cohen Act, Paperwork Reduction Act, Records Management, Chief Financial Officer, Standard Financial Information Structure, Section 508 of the Rehabilitation Act, interoperability, infrastructure, information collections, National Defense Authorization Act, Business Enterprise Architecture, Business Process Reengineering, Enterprise Service Program/Project and Enterprise Technical Program/Project. For Information Technology budget reporting, ITIPS includes the Budget Estimate Submission and Presidential Budget activities. ITIPS supports data flow via an interface to the DoD's Information Technology Portfolio Repository (DITPR) system. ITIPS also optimizes the information technology budget and compliance processes, enables automation to the fullest extent possible and provides robust analytical capabilities.

1.6.2. The ITIPS tool is utilized by all key stakeholders. Information Technology investment Program Managers utilize ITIPS to document compliance status and Information Technology Budget execution information for individual investments. Portfolio Owners and Managers utilize ITIPS to manage activities across their portfolio in regards to Capital Planning and Investment Control and Information Technology investment management processes. The SAF/CIO A6X staff utilizes the inherent data integration and analytics of ITIPS to simplify, improve and standardize portfolio management activities to deliver capabilities to Functional customers across the Air Force. The investment administrative stakeholders of Information Technology investments must have accounts in ITIPS in order to manage their programs and/or portfolios.

1.6.3. The newly formed Enterprise Information Technology (EIT) Council, Board, and Group as well as the Information Technology Governance Executive Board (ITGEB) and Group (ITGEG) perform portfolio and investment reviews using ITIPS to display and compare the statuses of Information Technology portfolios and investments in terms of cost, schedule, performance, budget, compliance, functionality and technology factors. These

activities support the Chief Information Officer's statutory responsibilities, aid in the elimination of duplicative Information Technology systems and provide greater insight on investments allocated to functional capabilities across the Air Force.

1.6.4. All equipment, interconnected systems or subsystems of equipment as defined by this publication as Information Technology investments (see Attachment 1) must be reported in ITIPS so that they can be reported in the Information Technology budget. Exceptions to reporting Information Technology investments are defined in accordance with the DoD Financial Management Regulation, 7000.14R, Volume 2B, Chapter 18, paragraph 180102.D. Specific guidance for data entry into ITIPS is distributed to the field each budget cycle from SAF/CIO A6X, Information Technology Budget Branch.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Chief, Information Dominance and Chief Information Officer, Office of the Secretary of the Air Force (SAF/CIO A6). SAF/CIO A6 conducts Portfolio Management and Capital Planning and Investment Control through the DoD decision support processes and the Chief Information Officer internal corporate processes. The internal processes are managed through the Information Technology governance forums of the Enterprise Information Technology (EIT) Council, Board, and Group as well as the Information Technology Executive Board and Group (ITGEB & ITGEG). Externally, the SAF/CIO A6 utilizes their role in the Defense Business Council, the Enterprise Senior Working Group (ESWG), the Capabilities Development Council (CDC) and the Capabilities Development Working Group (CDWG) to further conduct portfolio management. The SAF/CIO A6, through its directorates and internal corporate processes, shall:

2.1.1. Review the performance of the Air Force Information Technology portfolios and National Security Systems programs. Provide recommendations on the continuation, modification, or termination of cyberspace, Information Technology and/or National Security Systems programs or projects pursuant to 40 USC § 11315, 44 USC § 3506, 44 USC § 3541, et seq. (the Federal Information Security Management Act of 2002), 44 USC § 3603 and other applicable authorities. These reviews will, at a minimum, be conducted annually. **(T-0)**

2.1.2. Advocate for Air Force Information Technology interests as a co-principal representative with SAF/MG in the Defense Business Council for Defense Business System, and at the Enterprise Senior Working Group.

2.1.3. Serve as Department of the Air Force cyberspace/Information Technology Portfolio Manager in coordination with the operational, functional and resource management stakeholders.

2.1.4. Serve a voting member on the Capabilities Development Council and inform members of Portfolio Management/Capital Planning and Investment Control decisions or issues.

2.1.5. Establish and maintain Portfolio Management/Capital Planning and Investment Control standards for Information Technology compliance. Approve and manage performance metrics to measure progress and review metrics to continually assess current Information Technology investment performance.

2.1.6. Manage and set the Investment Review Panel battle rhythm.

2.1.7. Review and evaluate risk profile (see Air Force Instruction 17-101, *Risk Management Framework (RMF) for Air Force Information Technology*, paragraph 2.6.10 and A6.1.2.16 for general guidance on risk evaluations).

2.1.8. Establish a schedule (battle rhythm) to review all Mission Area Information Technology portfolios (and/or investments as needed) annually to evaluate the following:

2.1.8.1. Strategic alignment of planning, acquisition, development, implementation, operations and maintenance of Air Force information system investments (and corresponding budgets) that best support the Information Dominance Flight Plan and overall Air Force strategic goals.

2.1.8.2. Information Technology investment risk.

2.1.8.3. Performance measures/metrics of existing Information Technology investments and existing initiatives to develop a recommendation to the DoD decision support and Air Force corporate structure on selection, control or termination.

2.1.8.4. Information Dominance initiatives and investments within the Enterprise Information Technology portfolio.

2.2. Deputy Chief Management Officer & Office of Business Transformation (SAF/MG). SAF/MG shall:

2.2.1. Ensure defense business systems accountability and modernization in compliance with 10 USC § 2222. **(T-0)**

2.2.2. Chair and provide the secretariat functions for the Enterprise Senior Working Group. This working group provides oversight for data systems within the Air Force Business Mission Area in coordination with SAF/CIO A6's governance forums to ensure Information Technology investment planning and control is consistent with DoD and Air Force strategic plans and guidance.

2.2.3. Ensure data systems within Air Force Business Mission Area are enabled by sufficient business process reengineering and executable Doctrine, Organization, Training, Materiel, Logistics, Personnel and Facilities actions during development & modernization activities.

2.2.4. Coordinate the Air Force Business Mission Area roadmap with SAF/CIO A6 governance forums for transitioning business systems into the Joint Information Environment.

2.2.5. Serve as the approval authority for the certification of funds and Air Force business capabilities requirements development in the Business Capability Acquisition Cycle Solution Analysis and Functional Requirements Authority to Proceeds per DoD Instruction 5000.75.

2.3. Assistant Secretary of the Air Force for Acquisition (SAF/AQ). SAF/AQ shall:

2.3.1. Participate in Information Technology governance forums.

2.3.2. Work with SAF/CIO A6 to ensure Air Force cyber acquisition programs are consistent with the Information Dominance Flight Plan and the Air Force Enterprise Architecture developed by SAF/CIO A6.

2.3.3. Ensure the execution of Air Force acquisition and sustainment programs appropriately implements cyberspace and warfighting integration requirements, including, interoperability, reusability of application designs and promoting the adoption of Information Technology as common services and the Air Force common computing environment. These requirements will be implemented in accordance with Air Force Instruction 63-101/20-101, *Integrated Life Cycle Management*.

2.3.4. Ensure the acquisition program office Program Manager is responsible for cybersecurity of the weapon system, to include Information Technology interfaces and embedded computer hardware and software and has allocated sufficient resources to cybersecurity.

2.3.5. Ensure all acquisition programs plan and conduct robust developmental and operational cyber testing prior to system deployment including those required to demonstrate compliance with cybersecurity requirements established for the program to be authorized to operate.

2.3.6. Designate DoD/Air Force information systems that the Air Force Service Acquisition Executive has determined are critical to the direct fulfillment of military or intelligence missions as "applicable systems" in accordance with DoD Instruction 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks.* **(T-0)**

2.4. Assistant Secretary of the Air Force, Financial Management and Comptroller (SAF/FM). SAF/FM shall:

2.4.1. Coordinate, as required, on business case analysis and/or economic analysis supporting cyberspace requirements.

2.4.2. In accordance with 10 USC § 8022, approve and supervise all financial cyberspace programs to ensure compliance with finance and accounting standards. **(T-0)**

2.4.3. Participate in Information Technology governance forums.

2.5. Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance (AF/A2). AF/A2 shall:

2.5.1. Advocate for a prioritized integration of battlespace awareness warfighting systems and intelligence, surveillance and reconnaissance enterprise interoperability under the warfighting integration governance forums and with other appropriate forums as needed.

2.5.2. Participate in Information Technology governance forums.

2.5.3. Conduct review of Defense Intelligence capabilities and investments, including all Defense Intelligence Mission Area and those Intelligence, Surveillance and Reconnaissance systems aligned within Battlespace Awareness and Command, Control, Communications and Computers Intelligence, Surveillance and Reconnaissance.

2.5.4. Identify opportunities to share capabilities and investment between Defense Intelligence Mission Area and the other Mission Areas.

2.5.5. Ensure Air Force Defense Intelligence Mission Area portfolios properly implement Intelligence Community Directive 121, *Managing the Intelligence Community Information Environment* and Intelligence Community Directive 503, *Intelligence Community Information Systems Security Risk Management*. **(T-0)**

2.6. Chief, Information Dominance and Chief Information Officer, Office of the Secretary of the Air Force Cyberspace Capabilities and Compliance Directorate (SAF/CIO A6X). The SAF/CIO A6X shall:

2.6.1. Establish and maintain a coherent cyberspace/Information Technology Portfolio Management/Capital Planning and Investment Control management process for integrated, efficient and effective allocation of resources on Information Technology investments.

2.6.2. Publish standardized Portfolio Management/Capital Planning and Investment Control compliance guidance for all stakeholders.

2.6.3. Ensure the cyberspace/Information Technology Capital Planning and Investment Management process is integrated with planning, programming, budgeting, financial, strategic sourcing and program management processes.

2.6.4. Review Air Force budget requests for cyberspace/Information Technology and National Security Systems pursuant to 10 USC § 2223 and develop a full and accurate accounting (in coordination with SAF/FM) of Information Technology expenditures, related expenditures and results pursuant to 44 USC § 3506 and 40 USC § 11315. **(T-0)**

2.6.5. Ensure cyberspace/Information Technology investments are aligned with Air Force strategy and capability delivery in coordination with the operational and resource management stakeholders, as well as with all applicable laws, policies and regulations.

2.6.6. Ensure the elimination of duplicate cyberspace/Information Technology and National Security Systems within Air Force Information Technology portfolios.

2.6.7. Ensure Information Technology investments are properly registered into the Information Technology data repository ITIPS.

2.6.8. Serve as a voting member on the Capabilities Development Working Group, informing the other members of Portfolio Management/Capital Planning and Investment Control decisions/issues. Inform the Capabilities Development Council of Portfolio Management/Capital Planning and Investment Control decisions/issues.

2.6.9. Monitor and report information technology compliance (see paragraph 1.6.1.) with statutory and mandated requirements.

2.7. Information Technology Portfolio Owners. Portfolio Owners currently consist of MAJCOM/Core Function Leads, Headquarters Air Force and Secretariat of the Air Force staffs, and certain Combatant Command staffs that have Air Force Information Technology investments. With the stand-up of the Air Force Warfighting Integration Capability portfolio ownership responsibilities will transfer to the appointed Lead Command/Agency. A full list of current Portfolio Owners is listed in Attachment 7. The Information Technology Portfolio Owners shall:

2.7.1. Adhere to SAF/CIO A6 Portfolio Management/Capital Planning and Investment Control guidance in order to ensure uniformity in Capital Planning and Investment Control reporting.

2.7.2. Assign Portfolio Managers for portfolios within their control via appointment letter.

2.7.3. Assign Program and/or Project Managers via appointment letter for non-Program Executive Officer appointed Information Technology investment activities within their portfolio.

2.7.4. Validate that portfolio(s) provide DoD and Air Force mission capability and aligns with DoD and Air Force strategy, operational goals, Mission Areas and Functional capability areas.

2.7.5. Maintain a 12-month forecast of upcoming requirement and/or acquisition events for all programs in their portfolio.

2.7.6. Perform risk assessments for all programs within their portfolio in support of the Joint Capabilities Integration and Development System, Business Capability Acquisition Cycle or

Defense Acquisition System and Planning, Programming, Budgeting and Execution processes (DoD decision support processes).

2.7.7. Provide operational analyses of Information Technology investments to determine whether investments meet/maintain expected outcome, performance, return on investment and cost effectiveness.

2.7.8. Actively participate in DoD decision support processes as appropriate and integrate Portfolio Management/Capital Planning and Investment Control criteria as listed (interoperability, cybersecurity, Enterprise Architecture, strategy alignment, risk, Clinger-Cohen Act compliance, etc. see Attachment 6) into corporate process deliverables.

2.7.9. Conduct Post Implementation Reviews in accordance with Air Force Manual 17-1402, *Air Force Clinger-Cohen Act (CCA) Compliance Guide.*

2.7.10. Ensure Doctrine, Organization, Training, materiel, Leadership, Personnel and Facilities factors and/or options are considered through the acquisition process prior to proceeding with a materiel solution.

2.7.11. Work with Portfolio Managers to develop an effective Information Technology management program.

2.7.12. Track Business Mission Area system Organizational Execution Plan information for certification (if applicable).

2.7.13. Track Organizational Execution Plans certified programs and milestones to ensure expected benefits and outcomes are realized (if applicable).

2.7.14. Perform annual review of Information Technology investment information for accuracy and completeness.

2.7.15. Conduct annual Capital Planning and Investment Control reviews (see Attachment 6) of all Information Technology systems encompassed in their portfolio and ensure.

2.7.16. Ensure portfolio manager billets are properly coded as Information Technology level one acquisition professionals (at a minimum).

2.7.17. Track Information Technology compliance status for all investments in their portfolio.

2.7.18. Ensure Program Managers are advised of National Defense Authorization Act certification and Information Technology compliance requirements and are notified of requirement changes in the portfolio.

2.8. Portfolio Managers. The Portfolio Manager shall:

2.8.1. Serve as the advisor to a Program Manager and/or Project manager (if established).

2.8.2. Acquire Information Technology acquisition professional level one certification (at a minimum) through Defense Acquisition University and be familiar with the DoD budgeting process in order to perform Portfolio Management duties.

2.8.3. Actively participate in DoD decision support processes as appropriate and integrate Portfolio Management/Capital Planning and Investment Control criteria as listed in section

1.3 and Attachment 6 into requirement, acquisition and budgeting deliverables (as applicable).

2.8.4. Support the Portfolio Owner to ensure Information Technology Investments align to business strategy and objectives and support the elimination of duplicative investments.

2.8.5. Provide, at a minimum, an annual report on the overall health of the portfolio (compliance, performance, cybersecurity, funding, integration, traceability to Information Dominance Flight Plan and other areas addressed in Attachment 6) to the Portfolio Owner and Information Technology governance forums to support Capital Planning and Investment Control reviews.

2.8.6. Manage all Information Technology investments and compliance and financial data in accordance with SAF/CIO A6 and Information Technology governance forum directives within ITIPS.

2.8.7. Track Information Technology compliance status for all systems in their portfolio.

2.8.8. Annually review portfolio data within ITIPS for accuracy and completeness.

2.8.9. Assist the Portfolio Owner to ensure Doctrine, Organization, Training, materiel, Leadership, Personnel and Facilities factors and/or options are considered through the acquisition process prior to proceeding with a materiel solution.

2.8.10. Adhere to SAF/CIO A6 and Air Force Warfighting Integration Capability/MAJCOM Portfolio Management and Capital Planning and Investment Control guidance in order to ensure uniformity in Capital Planning and Investment Control reporting.

2.9. Program Managers/Project Managers. Since many Information Technology investments may not be acquired through a formally established program, the responsibilities of the Program Manager and Project Manager are grouped together. The Program and Project Managers shall:

2.9.1. Except for programs of record, prepare Information Technology business cases (see Attachment 6) and manage Information Technology investments in accordance with guidance from SAF/CIO A6 and associated best practices. For programs of record, Program Managers will conduct a business case analysis in accordance with Air Force Instruction 63-101/20-101.

2.9.2. For development, modernization, or enhancement projects, or those in mixed life cycle, use an appropriately compliant American National Standards Institute Standard 748 earned value management system to collect government earned value data and merge that data with the contractor's earned value data for a full picture of the Information Technology investment performance when applicable. For programs of record, earned value management (where required) will be addressed by the Program Manager per DoD Instruction 5000.02 or 5000.75.

2.9.3. For programs of record, perform an Integrated Baseline Review in accordance with DoD Instruction 5000.02 or 5000.75 requirements.

2.9.4. Conduct periodic Compliance and Surveillance Reviews to ensure the contractor's earned value management system is appropriately compliant with Electronic Industries Alliance 748 criteria and follows its guidelines. For programs of record, Compliance and

Surveillance Reviews will be addressed by the Program Manager per DoD Instruction 5000.02 or 5000.75.

2.9.5. Actively participate in DoD decision support processes as appropriate and integrate Portfolio Management/Capital Planning and Investment Control criteria as listed in section 1.3 and Attachment 6 into deliverables. For programs of record, all criteria will be addressed by the Program Manager per DoD Instruction 5000.02 or 5000.75.

2.9.6. Provide surveillance of contractors to ensure they are planning and controlling investment activities and providing timely and accurate reports. For programs of record, all contractor supervision will be addressed by the Program Manager per DoD Instruction 5000.02 or 5000.75.

2.9.7. Monitor the project to determine if assets are performing within baseline cost and are projected to meet schedule and performance goals. For programs of record, operational analyses will be addressed with an acquisition strategy by the Program Manager per DoD Instruction 5000.02 or 5000.75.

2.9.8. Register and enter applicable Information Technology investment, compliance and financial data in accordance with SAF/CIO A6 and Information Technology governance forum directives into ITIPS.

2.9.9. Generate information necessary to support the Air Force Organizational Execution Plans (for Business Mission Area systems).

2.9.10. Perform an annual review of Information Technology investment submissions in ITIPS for accuracy and completeness.

BRADFORD J.SHWEDO, Lt Gen, USAF
Chief, Information Dominance
and Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AF/A5R, *Requirements Development Guidebook*, Vol 1 & Vol 2, September 19, 2016

AFI 17-101, *Risk Management Framework (RMF) for Air Force IT*, February 2, 2017

AFI 17-140, *Air Force Architecting*, November 2, 2017

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

AFI 63-101/20-101, *Integrated Life Cycle Management*, May 9, 2017

AFI 65-509, *Business Case Analysis*, September 19, 2011

AFI 99-103, *Capabilities-Based Test and Evaluation*, April 6, 2017

AFMAN 17-1402, *Air Force Clinger-Cohen Act (CCA) Compliance Guide*, October 24, 2012

AFMAN 33-363, *Management of Records*, June 2, 2017

AFMAN 63-144, *Defense Business System Life Cycle Management*, March 31, 2016

AFPD 10-6, *Capability Requirements Development*, November 6, 2013

AFPD 10-9, *Lead Command Designation and Responsibilities for Weapon Systems*, March 8, 2007

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

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

American National Standards Institute/Electronic Industries Alliance 748, March 2013

CJCSI 3100.01C, *Joint Strategic Planning System*, November 20, 2015

CJCSI 3170.01I, *Joint Capabilities Integration and Development System*, January 23, 2015

CJCSI 5123.01G, *Charter of the Joint Requirements Oversight Council*, February 12, 2015

DoD Information Technology Portfolio Repository User's Guide, June 2011

DoDD 5000.01, *The Defense Acquisition System*, November 20, 2007

DoDD 5144.02, *DOD Chief Information Officer (DOD CIO)*, November 21, 2014

DoDD 5200.43, *Management of the Defense Security Enterprise*, August 15, 2017

DoDD 7045.14, *The Planning, Programming, Budgeting and Execution (PPBE) Process*, January 25, 2013

DoDD 8000.01, *Management of the Department of Defense Information Enterprise*, March 17, 2016

DoDD 8115.01, *Information Technology Portfolio Management*, October 10, 2005

DoD FMR, 7000.14R Volume 2B, *Department of Defense Financial Management Regulation*, December 2016

DoDI 5000.02, *Operation of the Defense Acquisition System*, January 7, 2015 incorporating change 1 January 26, 2017

DoDI 5000.74, *Defense Acquisition of Services*, January 5, 2016, Incorporating Change 1, October 5, 2017

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

DoDI 8115.02, *Information Technology Portfolio Management Implementation*, October 30, 2006

DoDI 8500.01, *Cybersecurity*, March 14, 2014

GAO Executive Guide, GAO-04-394G, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, March, 2004

HAF MD 1-26, *Chief, Information Dominance and Chief Information Officer*, February 5, 2015

JP 3-13, *Information Operations*, November 27, 2012 incorporating Change 1 November 20, 2014

OMB Circular A-130, *Management of Federal Information Resources*, July 27, 2016

OMB Memorandum M-11-29, *Chief Information Officer Authorities*, August 8, 2011

United States Code Title 40 Chapter 25 Subchapter 1 Part D Section 1452

United States Code Title 40 Subtitle III Chapter 113 Subchapter 2

United States Code Title 44 Chapter 35 Subchapter 1 Section 3506

Adopted Forms

Air Force Form 847, *Recommendation for Change of Publication*

Air Force Form 1067, *Modification Proposal*

Abbreviations and Acronyms

AFI—Air Force Instruction

AFMAN—Air Force Manual

CIO—Chief Information Officer

CDC—Capabilities Development Council

CDWG—Capabilities Development Working Group

CJCS—Chairman of the Joint Chiefs of Staff

DITIP—Defense Information Technology Investment Portal

DITPR—DoD's Information Technology Portfolio Repository

DoD—Department of Defense

EIT—Enterprise Information Technology

ESWG—Enterprise Senior Working Group

HAF—Headquarters Air Force

IT—Information Technology

ITGEB—Information Technology Governance Executive Board

ITGEG—Information Technology Governance Executive Group

ITIPS—Information Technology Investment Portfolio Suite

MAJCOM—Major Command

MD—Mission Directive

OMB—Office of Management and Budget

OPR—Office of Primary Responsibility

PPBE—Planning, Programming, Budgeting and Execution

SAF—Secretariat of the Air Force

SAF/AQ—Assistant Secretary of the Air Force for Acquisition

SAF/CIO A6—Chief of Information Dominance and Chief Information Officer

SAF/CIO A6X—Director of Cyberspace Capabilities and Compliance

SAF/FM—Assistant Secretary of the Air Force, Financial Management and Comptroller

SAF/MG—Director of Business Transformation and Deputy Chief Management Officer

SNaP-IT—Select & Native Programming Data Input System for Information Technology

Terms

Business Case Analysis—(Air Force Instruction 65-509) A business case analysis, also referred to as a business case or business plan, is a decision support document that identifies alternatives and presents business, economic, risk, and technical arguments for selecting an alternative to achieve organizational or functional missions or goals. Business case analyses do not replace the judgment of the decision maker, but rather aid that judgment by considering possible alternatives, their costs, benefits, and risks, and the degree to which they meet program objectives, or are either within budget constraints or require additional funding.

Business Mission Area—(DoD Instruction 8115.02) Ensures that the right capabilities, resources and materiel are reliably delivered to warfighters including: what they need, where they need it, when they need it, anywhere in the world. In order to cost-effectively meet these requirements, the DoD 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.

Capital Planning and Investment Control—Capital Planning and Investment Control is an integrated management process within Portfolio Management for the continuous selection, control and evaluation of Information Technology investments over their life cycles and is focused on achieving desired outcomes in support of the Air Force's missions, goals and objectives. According to 40 USC § 11312, Capital Planning and Investment Control should "maximize the value and assess and manage the risks, of…information technology acquisition."

The program should "provide for the selection of information technology investments… management… and evaluation of the results of the investments." It should also "be integrated with the processes for making budget, financial and program management decisions" already in place within the agency.

Control—Control**,** per DoD Instruction 8115.02, is "the activity focused on acquiring the capabilities selected for the portfolio. It consists of acquisition and oversight activities at the portfolio level that complement and supplement traditional single-system, single-platform acquisition and oversight activities."

Cybersecurity—As stated in Committee on National Security Systems Instruction 4009, the ability to protect or defend the use of cyberspace from cyber-attacks.

Cyberspace—A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems and embedded processors and controllers. (Joint Pub 3-12) NOTE: synonymous with cyber when used as an adjective.

Defense Business System—(DoD Instruction 5000.75) Defense Business Systems are information systems that are operated by, for, or on behalf of the DoD, 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 defense 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 DoD conducted for the morale, welfare and recreation of members of the armed forces using non-appropriated funds.

Defense Information Technology Investment Portal (DITIP)—Defense Information Technology Investment Portal is a DoD enterprise service providing a centralized location for all Information Technology Investment data and includes the capability to initiate, modify and retire Information Technology investments. The Defense Information Technology Investment Portal supports data requirements for the DoD Information Technology budget submission, Defense Business System investment review process, Information Technology systems inventory and future DoD Information Technology data requirements.

DoD's Information Technology Portfolio Repository (DITPR)—(DITPR Guidance) DoD's Information Technology Portfolio Repository is the Department's consolidated inventory of Information Technology systems. It provides comprehensive unclassified inventory of mission critical and mission essential DoD information systems as required by 10 USC 2223(a)(5) and DoDD 5144.02. The system contains information regarding DoD information systems required to be registered. This includes information such as system names, acronyms, descriptions, sponsoring component, approval authority, points of contact, and other basic information required for any analysis of Departmental inventory, portfolios, or capabilities.

Defense Intelligence Mission Area—(DoD Instruction 8115.02) Includes Information Technology investments within the Military Intelligence Program. The Under Secretary of Defense for Intelligence has delegated responsibility for managing the Defense Intelligence Mission Area portfolio to the Director, Defense Intelligence Agency, but the Under Secretary of Defense for Intelligence retains final signature authority. Defense Intelligence Mission Area

management will require coordination of issues among portfolios that extend beyond the Department of Defense to the overall Intelligence Community.

Evaluation—Evaluation, per DoD Instruction 8115.02, is the activity focused on measuring and assessing the outcomes of portfolio investments to determine whether expected benefits were achieved. Primary mechanisms for evaluation are Post Implementation Reviews and other operational assessments (e.g., after-action reports from military exercises). Evaluation results feed back into the other activities of Information Technology Portfolio Management to guide all investment decisions and recommendations.

Future Years Defense Program—The 5-year program and financial plan for the DoD, as approved by the Secretary of Defense and presented to Congress with the Presidential budget.

Information Environment—(Joint Publication 3-13) The aggregate of individuals, organizations and systems that collect, process, disseminate, or act on information. The information environment, which includes cyberspace, consists of three interrelated dimensions that continuously interact with individuals, organizations and systems. These dimensions are the physical, informational and cognitive, in accordance with Joint Publication 1-02 and Joint Publication 3-13.

Information Environment Mission Area—(DoD Instruction 8115.02) Represents, the common, integrated information computing and communications environment of the DoD Information Network (DoDIN). The Information Environment is composed of DoD Information Network assets that operate as, provide transport for and/or assure local area networks, metropolitan area networks and wide area networks. The Information Environment includes computing infrastructure for the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information, with primary emphasis on DoD enterprise hardware, software operating systems and hardware/software support that enable the DoD Information Network enterprise. The Information Environment also includes a common set of enterprise services, which provide awareness of, access to and delivery of information to the DoD Information Network.

Information System—(DoD Directive 8000.01) 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 and DoD Directive 8000.01, *Management of the Department of Defense Information Enterprise*, the term "**information technology**" is defined as "any services or 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 contractor use of that equipment to a significant extent in the performance of a service or the furnishing of a product to the executive agency. Information Technology 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."

Initiative—A collection of resources focused on a single Information Technology project. Initiatives include both new starts and ongoing efforts and that a single initiative, in the Information Technology budget reporting construct, may equate to a program/project (either acquisition or sustainment/legacy), a collection of related programs/projects, or a collection of related programs and activities focused on Information Technology.

Intelligence Planning, Programming, Budgeting and Execution—The process for National Intelligence, Surveillance and Reconnaissance Information Technology investments through Director of National Intelligence.

Information Technology Investment—An information technology investment per DoD Directive 8000.01, "may include a project or projects for the development, modernization, enhancement, or maintenance of a single Information Technology asset or group of Information Technology assets with related functionality and the subsequent operation of those assets in a production environment." All Information Technology investments should have a defined life cycle with start and end dates, with the end date representing the end of the currently estimated useful life of the investment, consistent with the investment's most current alternatives analysis if applicable. Information Technology investments include Platform Information Technology.

Information Technology Portfolio—Per DoD Directive 8115.01, an Information Technology portfolio is defined as a grouping of Information Technology investments by capability to accomplish a specific Functional goal, objective, or mission outcome.

Information Technology Services—(DoDI 5000.74) The performance of any work related to Information Technology and the operation of Information Technology, including National Security Systems. This includes outsourced Information Technology-based business processes, outsourced Information Technology and outsourced information functions.

Joint Capabilities Integration and Development System—(CJCSI 3170.01I) A Chairman of the Joint Chiefs of Staff process identifying, assessing, validating and prioritizing joint military capability requirements. The Joint Capabilities Integration and Development System process is a collaborative effort which uses joint concepts and DoD architectures to identify prioritized capability gaps and integrated Doctrine, Organization, Training, materiel, Leadership and Education, Personnel, Facilities-Policy solutions (materiel and non-materiel) to resolve those gaps.

Mission Area—(DoD Directive 8115.01) Defined areas of responsibility with functions, processes and capabilities that contribute to mission accomplishment.

National Security Systems (NSS)—National Security Systems, as defined in Title 44 USC 3552 (Reference (aw)), are telecommunications or information systems operated by or on behalf of the Federal Government, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or, is critical to the direct fulfillment of military or intelligence missions. National Security Systems do not include systems that are used for routine administrative and business applications (including payroll, finance and personnel management applications).

Platform Information Technology—AFPD 17-2 defines platform information technology as "a special purpose system which employs computing resources (e.g., hardware, firmware and optionally software) that are physically embedded in, dedicated to, or essential in real time to the

mission performance. It only performs (i.e., is dedicated to) the information processing assigned to it by its hosting special purpose system (this is not for core services)."

Portfolio Management—(DoD Instruction 8115.02) The management of selected groupings of Information Technology investments using strategic planning, architectures and outcome-based performance measures to achieve a mission capability. The outcome-based performance measures are addressed through meeting Capital Planning and Investment Control execution requirements.

Program Objective Memorandum—The final product of the programming process within the DoD, the DoD Component's Program Objective Memorandum displays the resource allocation decisions of the Military Departments in response to and in accordance with planning and programming guidance.

Program of Record—1) Program as recorded in the current Future Years Defense Program or as updated from the last Future Years Defense Program by approved program documentation (e.g., Acquisition Program Baseline (APB), acquisition strategy, or Selected Acquisition Report (SAR)). If program documentation conflicts with latest Future Years Defense Program, the Future Years Defense Program takes priority. 2) May also refer to a program having successfully achieved formal program initiation, normally Milestone B.

Program Budget Review—The Program Budget Review is an annual review coordinated by the Office of the Under Secretary of Defense (Comptroller) (USD(C)) and Office of the Secretary of Defense CAPE to facilitate consolidation of program objective memorandums and Budget Estimate Submissions from the Services and other DoD Components and adjudication of any outstanding issues before presenting the overall DoD Program Objective Memorandum/Budget Estimate Submission input to the Presidential budget submission. The Program Budget Review provides key opportunity to ensure that budgetary decisions are fully informed by the priorities of the validated capability requirements of the Joint Force.

Selection—Selection is the activity that identifies the best mix of investments within available resources to meet integrated enterprise, Mission Area, subportfolio and Air Force strategic goals. Portfolio selection decisions are made using integrated architectures, transition plans, technical criteria and programmatic trade-offs to satisfy performance measures and achieve desired outcomes.

Select & Native Programming Data Input System for Information Technology (SNaP-IT)—is the authoritative database application used by the DoD Chief Information Officer to collect, coordinate, publish and disseminate the DoD Information Technology Budget and DoD Cyberspace Operations Budget to meet requirements established by the Congress and the Office of Management and Budget.

Sponsor (Joint Capabilities Integration and Development System)—Per the Air Force Requirements Development Guidebook Vol 1, 19 Sep 2016, sponsors are the ones who 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 must use formal capabilities-based processes to identify, evaluate, develop, field and sustain capabilities that compete 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.

Warfighting Mission Area—(DoD Instruction 8115.02) The Warfighting Mission Area provides life cycle oversight to applicable DoD Component and Combatant Commander Information Technology investments (programs, systems and initiatives). Warfighting Mission Area Information Technology investments support and enhance the Chairman of the Joint Chiefs of Staff's joint warfighting priorities while supporting actions to create a net-centric distributed force, capable of full spectrum dominance through decision and information superiority.

Attachment 2

WARFIGHTING MISSION AREA CATEGORIZATION CRITERIA AND RATIONALE

Figure A2.1. Warfighting Mission Ara Categorization Criteria and Rationale.

Mission Readiness Support Systems	Systems that support mission readiness should be categorized as Warfighting Mission Area or Defense Intelligence Mission Area
Research and Development Systems	Systems that support research and development should be categorized as Warfighting Mission Area, Defense Intelligence Mission Area or Business Mission Area. Information Technology investment uniquely identified as Science and Technology (S&T) or Developmental Test and Evaluation (DTE) and do not directly support a business function are Warfighting Mission Area.
National Security Systems	Systems which: (1) involve command and control of military forces; (2) involve equipment that is an integral part of a weapon or weapons system

Attachment 3

BUSINESS MISSION AREA CATEGORIZATION CRITERIA AND RATIONALE

Figure A3.1. Business Mission Area Categorization Criteria and Rationale.

Case Management System	If the system is a Case Management system for business information, it should be categorized as Defense Business System in Business Mission Area.
Financial Management System	If the system is a Financial Management System for business information, it should be categorized as Defense Business System in Business Mission Area
Human Resource Management System	If the system is a Human Resource Management System for business information, it should be categorized as Defense Business System in Business Mission Area
Knowledge Management System	If the system is a Knowledge Management System for business information, it should be categorized as Defense Business System in Business Mission Area
Logistics Systems	If the system is a Logistics System for business information, it should be categorized as Defense Business System in Business Mission Area
Management Systems	Management systems used for tracking and reporting of business information at DoD agencies should be categorized as Defense Business System in the Business Mission Area.
Records Management Systems	Records Management Systems and Workflow Management for business Information should be categorized as Defense Business System in the Business Mission Area.
Support Business Management Systems	Supporting Business Management Systems/functions (tasks, correspondence management, foreign disclosure, Freedom of Information Act, postal, public communications, inspection, audit, survey, project management and physical access control) should be categorized as a Defense Business System in Business Mission Area.
Acquisition Support Systems	If the system is a Acquisition Support System for business information, it should be

	categorized as Defense Business System in Business Mission Area
Business Security Systems	Systems that support business aspects of security (such as those in the Defense Security Enterprise (see DoD Directive 5200.43) should be categorized as Defense Business System in Business Mission Area
Research and Development Systems	Systems that support research and development should be categorized as Warfighting Mission Area, Defense Intelligence Mission Area or Business Mission Area. Questions that may help determine if the R&D system falls within Business Mission Area are listed below: Does the Information Technology investment support a business operation, function, or activity which meets the definition of a Defense Business System? Does the investment used to support a business operation, function, or activity meet the definition of an information system, as defined in title 44 USC section 3502? Does the Information Technology investment rely on other Defense Business Systems for interoperability? Does the Information Technology investment rely on a level of adherence to the BEA to effectively guide, constrain and permit interoperable Defense Business Systems solutions or support the governance framework for Defense Business Systems? Does the Information Technology investment involve inherently managerial functions or provide business functions or capabilities such as strategic planning, case/correspondence/records management, project or program management, or other staff functions performed at a management headquarters level?

Attachment 4

INFORMATION ENVIRONMENT MISSION AREA CATEGORIZATION CRITERIA AND RATIONALE

Figure A4.1. Information Environment Mission Area Categorization Criteria and Rationale.

Portals and Intranets	Generic – Information Environment Mission Area If the system is a generic portal capability (e.g., out-of-the box SharePoint, Livelink or similar), or intranet capability that provides basic file sharing, calendar and workflow, without custom applications, then it should be categorized as Information Environment Mission Area. Complex Capability – Support Mission Area If the system has custom application(s) built on a portal or intranet capability that provide significant functionality to support a mission area, then it should be categorized as the corresponding non-Information Environment Mission Area.
Websites	Static Websites with little or no system functionality should be categorized as Information Environment Mission Area.
Information Technology Asset Management (ITAM)/Information Technology Service Management (ITSM)	Systems that support ITAM/ITSM processes should be categorized as Information Environment Mission Area
System Engineering Life-cycle Support (SELC)	SELC – Information Environment Mission Area Systems that support the Systems Engineering Lifecycle (e.g., architecture, requirements, software development, configuration, test and project management) should be categorized as Information Environment Mission Area. SELC support systems that are embedded within non-Information Environment Mission Area programs of record, should not be separately categorized or reported.

Attachment 5

DEFENSE INTELLIGENCE MISSION AREA CATEGORIZATION CRITERIA AND RATIONALE

Figure A5.1. Defense Intelligence Mission Area Categorization Criteria and Rationale.

National Security Systems	Systems which: (1) involve intelligence activities; (2) involve cryptologic activities related to national security; (3) is critical to the direct fulfillment of military or intelligence missions (that is not used for routine administrative and business applications (including payroll, finance, logistics and personnel management applications)).
Research and Development Systems	Systems that support research and development should be categorized as Warfighting Mission Area, Defense Intelligence Mission Area or Business Mission Area. Questions that may help determine if the R&D system falls within Defense Intelligence Mission Area are listed below: Does the Information Technology investment include investments within the Military Intelligence Program? Does the Information Technology investment involve intelligence or cryptologic activities related to national security?

Attachment 6

CAPITAL PLANNING AND INVESTMENT CONTROL QUESTIONNAIRE

A6.1. *"Select"* Phase Questions directed by Office of Management and Budget A-130.

A6.1.1. Perform business case analyses for Information Technology investments using the DoD Information Technology Business Case Analysis template that are tailored according to the investment's scope. The DoD Information Technology Business Case Analysis is available on the DoD Chief Information Officer Portal.

A6.1.2. Have an investment selection process and associated criteria. Recommended general questions regarding the proposed Information Technology investment or solution are as follows.

A6.1.2.1. Does it support a core Mission Area(s) or capability requirement that needs to be performed by the Air Force/DoD?

A6.1.2.2. Does it fill a performance capability gap in achieving strategic goals and objectives with the maximum benefits at the lowest life cycle cost among viable alternatives?

A6.1.2.3. Is the Information Technology investment or solution being undertaken because no alternative private sector or government source can more efficiently support the function?

A6.1.2.4. Is the Information Technology investment being proposed because there is not a similar solution already available or with minimum redesign or reconfiguration?

A6.1.2.5. Is the Information Technology investment unique or a potential enterprise solution?

A6.1.2.6. How far along is the project system, or initiative in defining the future state and developing the transition plan from the current state?

A6.1.2.7. What are the plans to transition to the future state?

A6.1.2.8. Are there funding commitments for the life cycle of this Information Technology investment? Consider appropriations and Fiscal Years specific to their purpose.

A6.1.2.9. Does the Information Technology investment support work processes that have been simplified or otherwise redesigned to reduce costs, improve effectiveness, make best use of commercial off-the-shelf technology and enable secure information exchange and resource sharing?

A6.1.2.10. Does it demonstrate a projected best value, based on an analysis of quantifiable and qualitative benefits and costs and projected return on investment, which is clearly equal to or better than alternative uses of available public resources?

A6.1.2.11. Is the Information Technology investment consistent with applicable federal and DoD Information Enterprise and Air Force Enterprise Architecture?

A6.1.2.12. Does the proposed Information Technology investment or solution support the Air Force's work process? Do information flows integrate or align with DoD and Air Force strategic goals?

A6.1.2.13. Does the Information Technology investment or solution reflect the DoD Mission Areas' or Functional capability areas' technology direction?

A6.1.2.14. Does the Information Technology investment or solution adhere to standards that enable information exchange and resource sharing, while retaining flexibility in the choice of suppliers and in the design of local work processes?

A6.1.2.15. Are there other investments related to or dependent upon the investment? How will decisions about this investment affect those other investments?

A6.1.2.16. Determine if risk has been reduced by employing measures such as:

A6.1.2.16.1. Avoiding or isolating custom-designed components to minimize the potential adverse consequences on the overall project.

A6.1.2.16.2. Using fully tested pilots, simulations, or prototype implementations before going into production.

A6.1.2.16.3. Establishing clear measures and accountability for project progress.

A6.1.2.16.4. Securing substantial involvement and buy-in throughout the project from the program officials who will use the system.

A6.1.2.17. Does it employ an acquisition strategy that allocates risk between government and contractor, effectively uses competition, ties contract payments to accomplishments and takes maximum advantage of commercial technology?

A6.1.2.18. Have potential funding constraints been identified and considered?

A6.1.2.19. What is the expected return on investment for the investment or initiative?

A6.1.2.20. Have the ramifications of declining to fund certain investments or initiatives been given careful consideration?

A6.1.2.21. Have all opportunities to invest in crosscutting investments or initiatives been appropriately evaluated?

A6.1.2.22. Does the investment conflict, overlap with, or is it redundant with other projects or initiatives?

A6.1.2.23. Are the project owners capable of successfully executing the chosen Information Technology portfolio (i.e., are the appropriate resources available to complete the included investments or initiatives)?

A6.1.2.24. Does the investment or initiative make best use of commercial-off-the-shelf software, cloud computing and shared services?

A6.2. *"Control"* Phase Questions directed by Office of Management and Budget A-130.

A6.2.1. Annually perform a review of Information Technology investments addressing the criteria listed in the Select phase to ensure compliance and document changes.

A6.2.2. Ensure Information Technology investments remain consistent with federal, DoD and Air Force Enterprise Architecture.

A6.2.3. Address what pitfalls the Information Technology investments might encounter (e.g., events that could lead to poor outcomes) or have already encountered.

A6.2.4. Conduct a comparison of projected and realized outcomes and how they relate to pitfalls that have occurred for:

A6.2.4.1. Cost. Is the cost of investments within budget of the initial contract award? Is the cost of investments within budget of the overall projected contract value at time of award? Is there under-spending of resources with no schedule variance?

A6.2.4.2. Schedule. Determine the percentage of deliverables delivered on time each quarter. Address project schedule changes and impacts.

A6.2.4.3. Performance. Are investments delivering the anticipated return on investment?

A6.3. *"Evaluation"* Phase Questions directed by Office of Management and Budget A-130.

A6.3.1. Annually perform operational analyses for Major Information Technology investments that address whether investments meet/maintain expected criteria and how that relates to pitfalls that have occurred including outcomes (cost, schedule, performance and return on investment), efficiency/cost-effectiveness, support for requirements (including capability) and business needs.

A6.3.2. Determine a recommendation to continue, accelerate, decelerate, suspend or terminate an investment.

A6.3.3. Make use of post-implementation reviews.

A6.3.4. Develop and obtain Information Technology Governance Executive Group and/or Information Technology Governance Executive Board approval (as applicable) of disposition plans for each terminated or retired investment that addresses cessation and reallocation of Information Technology assets and funds and is in accordance with appropriate DoD records management, security and other Information Technology information management policies.

Attachment 7

AIR FORCE INFORMATION TECHNOLOGY PORTFOLIO OWNER LIST

Air Combat Command (ACC)
Air Education and Training Command (AETC)
Air Force District of Washington (AFDW)
Air Force Global Strike Command (AFGSC)
Air Force Material Command (AFMC)
Air Force Operational Test and Evaluation Center (AFOTEC)
Air Force Reserve Command (AFRC)
Air Force Space Command (AFSPC)
Air Force Special Operations Command (AFSOC)
Air Mobility Command (AMC)
Air National Guard (ANG)
Deputy Chief of Staff, Air and Space Operations (AF/A3)
Deputy Chief of Staff, Intelligence Surveillance and Reconnaissance (AF/A2)
Deputy Chief of Staff, Logistics, Engineering, and Force Protection (AF/A4/7)
Deputy Chief of Staff, Manpower, Personnel & Services (AF/A1)
Deputy Chief of Staff, Strategic Plans and Requirements (AF/A5/8)
Deputy Chief of Staff, Studies, Analyses, and Assessments (AF/A9)
North American Aerospace Defense Command (NORAD)
Pacific Air Forces (PACAF)
Secretary of the Air Force, Acquisition (SAF/AQ)
Secretary of the Air Force, Information Dominance & Chief Information Officer (SAF/CIO A6)
Secretary of the Air Force, Financial Management and Comptroller (SAF/FM)
Secretary of the Air Force, Administrative Assistant (SAF/AA)
United States Air Force Academy (USAFA)
United States Air Forces in Europe (USAFE)
U.S. Central Command (CENTCOM)
U.S. Northern Command (NORTHCOM)
U.S. Transportation Command (TRANSCOM)
U.S. Strategic Command (STRATCOM)