BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-141

23 DECEMBER 2008

Communications and Information

AIR FORCE INFORMATION TECHNOLOGY PORTFOLIO MANAGEMENT AND IT INVESTMENT REVIEW

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/XCPR

Certified by: SAF-XCP-2
(Brigadier General Ronnie D. Hawkins)
Pages: 20

This instruction implements Air Force Policy Directive (AFPD) 33-1, *Information Resources Management*. It establishes the guidelines, policies, and procedures for approving and managing Air Force Information Technology (IT) including National Security Systems (NSS), and implements guidance from 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*; Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 8410.01, *Warfighting Mission Area Information Technology Portfolio Management and Net-Centric Data Sharing; Department of Defense Directive (DoDD) 5134.3, Director of Defense Research and Engineering (DDR&E;)* Department of Defense Directive (DoDD) 8115.02, *Information Technology Portfolio Management*; Department of Defense (DoD) 7000.14-R, Volume 2B, *Department of Defense Financial Management Regulation (FMR);* and DoD Instruction (DoDI) 8115.02, *Information Technology Portfolio Management Implementation*. Send recommended changes or comments to Headquarters Air Force Communications Agency (HQ AFCA/EASD), 203 W. Losey St., Room 1100, Scott AFB IL 62225-5222, through appropriate channels, using Air Force (AF) Form 847, **Recommendation for Change of Publication**, with an information copy to Secretary of the Air Force (SAF/XCPR), 1800 Air Force Pentagon, Washington DC 20330-1800. 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 and disposed of in accordance with the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at https://www.my.af.mil/gcss-af61a/afrims/afrims/rims.cfm. See Attachment 1 for a glossary of references and supporting information.

Information Technology Portfolio Management has three main goals: maximize the value of the portfolio against the objectives of DOD; balance the portfolio; link the portfolio to strategy. To maximize the value of the portfolio, DOD will use financial analysis and scoring to prioritize the systems and initiatives in the DOD portfolio. By taking the approach of balancing the portfolio, DOD will look at the benefit vs. risk. Linking to DOD strategy is vital in order to correlate the dod strategic fit to resource allocation. The Portfolio Management process consists of binning, criteria determination, analysis, selection, control, and evaluation. These processes will result in recommendations that are carried out in JCIDS, the Defense Acquisition System and Planning, Programming, Budgeting & Execution (PPBE).

Chapter 1

AIR FORCE INFORMATION TECHNOLOGY PORTFOLIO MANAGEMENT

1.1. Background

1.1.1. Information Technology (IT) investments shall be managed as portfolios to: ensure IT 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. Most of the portfolio shall be managed using the Global Information Grid (GIG) architecture, plans, risk management techniques, capability goals and objectives, and performance measures. In addition, some Research, Development, Testing and Evaluation (RDT&E) activities will be conducted on the Defense Research & Engineering Network (DREN), in a stand alone environment, or in non-.mil network enclaves.

1.1.2. Portfolios shall be binned and integrated at the DoD Mission Area and Functional levels. 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) or capability areas that represent common collections of related, or highly dependent, system capabilities and services. Specifically, the SAF/XC Mission Area portfolios are defined as Warfighting, Business, Infrastructure, Force Development and Cyber Transformation.

1.1.3. Portfolios shall be used as a management tool in each of the Air Force's decision support systems including: Joint Capabilities Integration and Development System (JCIDS), DAS, Capabilities Risk Review Assessment (CRAA) and PPBE. Mission Area leads shall provide portfolio recommendations to the appropriate officials (Designated Approval Authorities) for consideration in the Air Force's decision support systems.

1.1.4. All authorities addressed in the Roles and Responsibilities Section of this document or instruction shall manage their portfolios by performing the following core functions:

1.1.4.1. Analysis. Links portfolio objectives to DoD/Air Force Enterprise vision, mission, goals, objectives, and priorities; develops quantifiable outcome-based performance measures; identifies capability gaps, opportunities, and redundancies; identifies risks; and provides for continuous process improvement.

1.1.4.2. Selection. Identifies and selects the best mix of IT investments to strengthen and achieve capability goals and objectives for the portfolio to ensure efficient and effective delivery of capabilities to the Warfighter, and to maximize return on investment to the Enterprise and demonstrates the impact of alternative IT investment strategies and funding levels.

1.1.4.3. Control. Ensures a portfolio is managed and monitored using established program management principles and quantifiable outcome-based performance measures. Portfolios are monitored and evaluated against portfolio performance measures to determine whether to recommend continuation, modification, or termination of individual investments within the portfolio.

1.1.4.4. Evaluation. Measures actual contributions of the 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 portfolio investments, as necessary

1.1.5. Governance forums shall be leveraged or established to manage portfolios, subportfolios, or capability areas at the Mission Area and Functional levels including hierarchically accountable subordinate levels of the portfolios at MAJCOMS, Agencies or Centers.

1.1.5.1. EITDR. Enterprise Information Technology Data Repository (EITDR) will be used as the governance tool for the AF CIO.

1.2. General:

1.2.1. This instruction implements policy and assigns responsibilities for the management of Air Force IT investments, including National Security System (NSS), and its associated resources as portfolios within the Air Force Enterprise that focus on improving Air Force and DoD capabilities and mission outcomes. It provides fundamental concepts for managing a portfolio of IT resources and defines processes for complying with external and internal statutory and regulatory requirements.

1.2.2. This instruction establishes a management framework to develop IT portfolios in each major command (MAJCOM), within Combatant Commands in which the Air Force expends IT resources, across the Headquarters Air Force (HAF), and the Secretary of the Air Force (SAF) functional staffs (see Attachment 2). This instruction also provides guidance on how the content of these portfolios will be documented to support the Air Force IT Portfolio Management (PfM) and decision-making processes in the Office of Warfighting Integration and Chief Information Officer (CIO), corporate structure, MAJCOM, Combatant Commands, HAF and SAF functional areas, and within the General Officer Steering Groups (GOSGs).

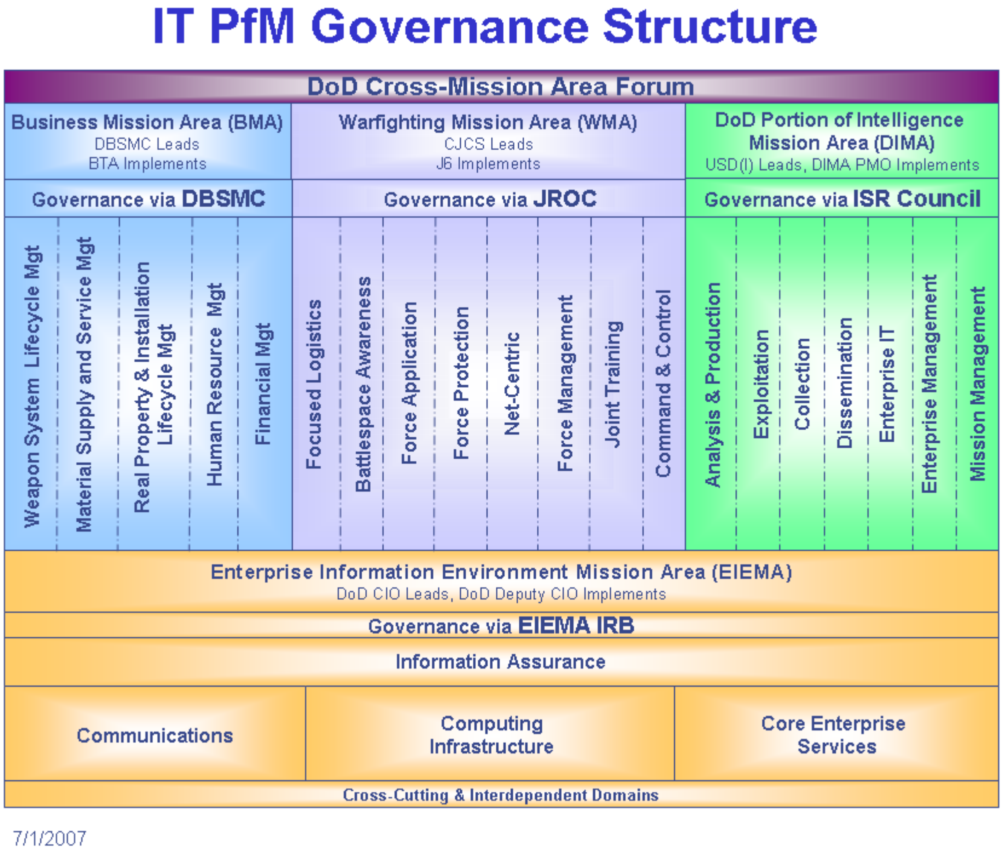
1.2.3. This instruction outlines requirements for identifying and registering IT resources (initiatives, systems, programs, projects, organizations, payments, and families of systems) within the Air Force EITDR. Guidelines for using the repository are included along with responsibilities for updating and maintaining the data stored therein. Roles and responsibilities for maintaining the repository, promulgating policy, defining and satisfying user requirements, and accounting for funding are also established.

1.3. Applicability and Scope. This instruction applies to all Air Force, Air National Guard, and Air Force Reserve IT resources (as defined in the definition section in the end of this instruction). Adherence is mandatory, except when statutory requirements, DoD or Joint Staff directives override. Refer specific interpretation queries to SAF/XCP.

1.4. Governance:

1.4.1. DoD policy directs the nesting and integration of portfolios at the Enterprise, Mission Area, and Component levels. The DoD Enterprise portfolio is divided into Mission Area portfolios, defined as Warfighting Mission Area (WMA), Business Mission Area (BMA), DoD portion of Intelligence Mission Area (DIMA), and Enterprise Information Environment Mission Area (EIEMA). Mission Area and Component portfolios may be divided into subportfolios (e.g., domains) or capability areas that represent common collections of related, or highly dependent, information capabilities and services. Figure 1.1 depicts the governance structure and Enterprise and Mission Area authorities to perform portfolio management in DoD and/or to define subportfolios or Component portfolios.

Figure 1.1. DoD IT PfM Governance Structure with Those Identified in 1.4.2.



IT PfM Governance Structure

DoD Cross-Mission Area Forum

Business Mission Area (BMA)
DBSMC Leads
BTA Implements

Governance via DBSMC

Weapon System Lifecycle Mgt | Material Supply and Service Mgt | Real Property & Installation Lifecycle Mgt | Human Resource Mgt | Financial Mgt

Warfighting Mission Area (WMA)
CJCS Leads
J6 Implements

Governance via JROC

Focused Logistics | Battlespace Awareness | Force Application | Force Protection | Net-Centric | Force Management | Joint Training | Command & Control

DoD Portion of Intelligence Mission Area (DIMA)
USD(I) Leads, DIMA PMO Implements

Governance via ISR Council

Analysis & Production | Exploitation | Collection | Dissemination | Enterprise IT | Enterprise Management | Mission Management

Enterprise Information Environment Mission Area (EIEMA)
DoD CIO Leads, DoD Deputy CIO Implements

Governance via EIEMA IRB

Information Assurance

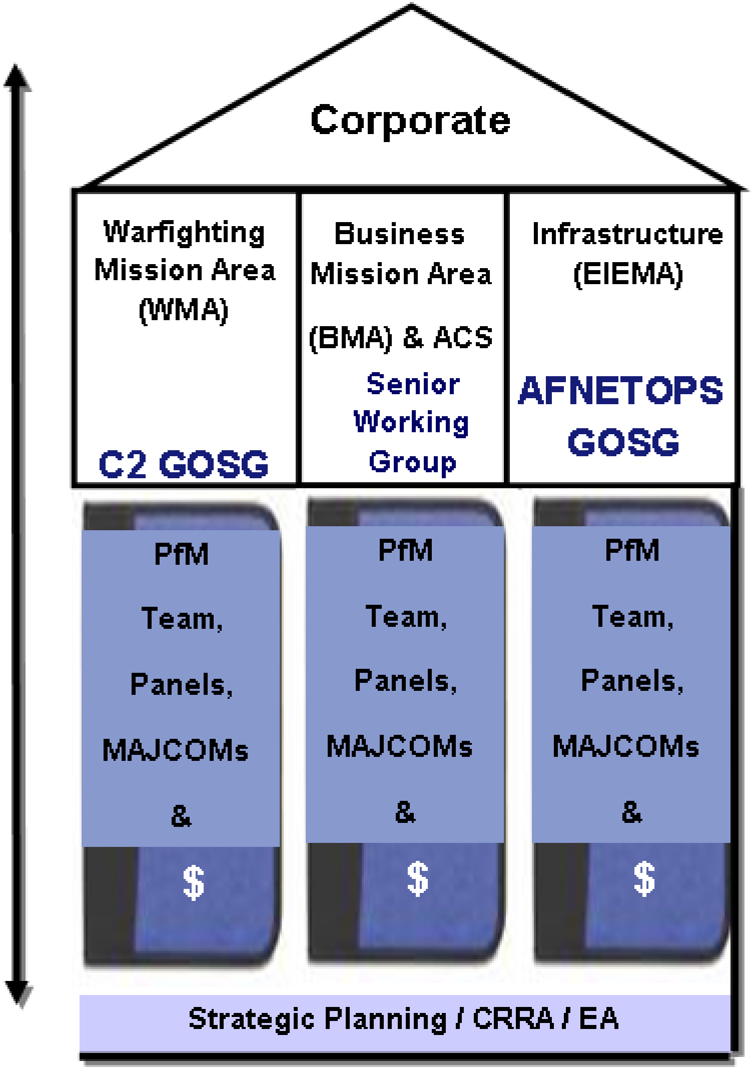
Communications | Computing Infrastructure | Core Enterprise Services

Cross-Cutting & Interdependent Domains

7/1/2007

1.4.2. The Air Force established GOSGs as the governing bodies for three of the sub-enterprise portfolios that align with the DoD Mission Areas. The GOSG is the decision body providing guidance and direction to the sub-enterprise portfolio. It provides the forums where MAJCOM Vice-commanders and Numbered Air Force commanders come to discuss solutions to key issues in all areas within these portfolios. Figure 1.2 depicts the governance structure with Authorities for these three sub-enterprise portfolios. Specifically, SAF/XC has established five mission areas in order to align with DoD policy and DoD enterprise portfolios. Those mission areas: Warfighter Networking, Business Capabilities and Agile Combat Support, Infrastructure, Cyber Transformation, and Force Development each correspond with the mission areas identified in Figure 1.1 minus the Cyber Transformation and Force Development mission areas which are SAF/XC specific.

Figure 1.2. Governance Structure with Authorities for Air Force Sub-Enterprise Portfolio.


Corporate
Warfighting Mission Area (WMA)
C2 GOSG
Business Mission Area (BMA) & ACS
Senior Working Group
Infrastructure (EIEMA)
AFNETOPS GOSG
PfM Team, Panels, MAJCOMs & $
PfM Team, Panels, MAJCOMs & $
PfM Team, Panels, MAJCOMs & $
Strategic Planning / CRRA / EA

1.4.2.1. Within each GOSG, a similar organizational structure will be utilized. Each GOSG will establish an Integrated Process Team (IPT) to maintain oversight of the resources associated with the portfolio. For example, SAF/XCP will act as a representative on the "Resources" IPT and will work closely with the other SAF/XC divisions with direct interaction with the GOSG structure. SAF/XCD will be a key player in the development and oversight of the Infrastructure architecture. SAF/XCD will ensure that programs within the Infrastructure portfolio are properly documented and aligned with the architecture. Likewise, SAF/XCT will do the same for the Business & Agile Combat Support (ACS) portfolio.

1.5. Roles and Responsibilities

1.5.1. SAF/XC is the Air Force CIO (AF CIO) and provides oversight, policy, and guidance for the Air Force IT Portfolio management community. The AF CIO serves as the Air Force IT enterprise portfolio manager for the Secretary of the Air Force (SECAF), with oversight responsibility for all Air Force IT in accordance with Public Law (PL) 104-106, *Clinger-Cohen Act of 1996*. SAF/XC ensures Air Force compliance with all regulatory and statutory directives and reporting requirements, and serves as the focal point and release authority for all Air Force IT reporting. The SAF/XC also serves as the chair or co-chair on each of the GOSGs.

1.5.2. SAF/XCP (Policy, Planning, and Resources). SAF/XCP implements strategy, plans, policy, governance, architectures, standards, resources, and investment strategy guidance based on an enterprise IT portfolio.

1.5.2.1. The SAF/XCP staff will act as Policy, Planning, & Resources Subject Matter Experts (SME) in support of the GOSGs as appropriate. The staff plans, oversees, and coordinates Air Force IT Portfolio management data-collection activities, and provides training and direction as appropriate. Additionally, the staff develops Air Force IT portfolio management policy, serves as Air Force liaison to OSD Networks and Information, Integration (OSD NII) on IT portfolio management topics and disseminates guidance and policy received from DoD and other external agencies to IT portfolio managers.

1.5.3. IT Portfolio Owners. MAJCOM Commanders & their associated Direct Reporting Units (DRUs), Combatant Commanders, and SECAF and CSAF organizational lead their respective IT portfolios. Portfolio owners have oversight responsibility for IT initiatives and systems for which they have lead funding responsibility. However, it is not necessarily the case that all IT portfolio resources fall within the portfolio owner’s organizational budget. Air Force IT portfolio owners are required to certify to SAF/XC, annually, that the IT Portfolio management information they provide is complete, accurate, and in accordance with current Air Force IT Portfolio management direction as provided in budgetary documents (policy, Annual Planning and Programming Guidance, Program Objective Memorandum Preparation Instructions, etc.).

1.5.4. IT Functional Portfolio Managers. MAJCOM, Combatant Command, SAF, HAF DRUs and HAF functional area CIOs (or equivalents) serve as their respective organizational portfolio manager, and support Air Force IT portfolio management data collection and reporting activities. The HAF and HAF DRUs CIO(s) or equivalents act as the IT Functional Portfolio Manager for initiatives within the HAF portfolio that are owned by HAF/IM (Director, Information Management for Headquarters Air Force and Headquarters Air Force Chief Information Officer). IT Functional Portfolio Managers advise and assist the IT Portfolio Owners in establishing and executing processes and procedures to meet all Air Force IT portfolio management requirements.

1.5.4.1. IT Functional Portfolio Managers must continue to support and interact with the HAF organizations that have functional oversight responsibilities. Portfolio management processes and information must be integrated with existing functional area responsibilities. This instruction does not preclude HAF functional area direction and guidance.

1.5.5. IT Portfolio Management Points of Contact (POCs). Each IT Functional Portfolio Manager will designate an IT Portfolio Management POC(s) for their respective organization. IT Portfolio Management POCs are responsible for communicating SAF/XC and SAF/AQ guidance and direction to their IT program/project managers, organizational Information System Security Officer (ISSO), financial program/project managers, and others responsible for IT portfolio management data collection and maintenance and partnering with them to collect and manage IT portfolio management data to support Air Force IT portfolio management and other processes.

1.5.5.1. Within their IT portfolio, each IT Portfolio Management POC(s) supports data review and validation, oversees and administers organizational IT portfolio management data collection and submission, and provides supplemental policy and guidance as required. IT Portfolio Management POCs review, validate, and coordinate all proposed initiative and system registration changes (additions, archivals, transfers between portfolios, or other significant modifications). IT Portfolio Management POCs are the approval authority for submitting any validated data updates and/or change requests to SAF/XC and SAF/AQ. In this role, IT Portfolio Management POCs shall coordinate these

changes closely with their associated IT Functional Portfolio Manager, Information Assurance (IA) POCs and other stakeholders as necessary.
1.5.6. Program Managers review and correct all budget and PM detail and maintain supporting documentations. Periodically review EITDR data for accuracy and completeness.

1.6. Air Force IT Portfolio Management Processes
1.6.1. IT portfolio management encompasses many processes based on executive, legislative, DoD and Air Force requirements. Lead responsibilities for these portfolio management processes and functions are distributed throughout the SAF/XC organization. For example: Federal Information Security Management Act of 2002 (FISMA) reporting is managed by SAF/XCPP; IT Lean Reengineering is managed by SAF/XCPP, Ronald Regan National Defense Authorization Act (NDAA) certification is managed by SAF/XCPP, IT budget exhibit reporting is managed by SAF/XCPR.
1.6.2. For portfolio management and reporting purposes, each IT portfolio within each of the sub-enterprise portfolios, is subdivided by IT Portfolio Owner. The IT Functional Portfolio Managers serve as the portfolio managers for these portfolios. The MAJCOM Vice Commanders (CVs) and functional representatives to the GOSG act as the IT portfolio owner's representatives for their respective portfolios.
1.6.3. Each Air Force IT investment shall be mapped to an initiative in the Air Force enterprise IT portfolio. Except for defense business system, initiatives may include more than one system, or may include a combination of system and non-system resources. Non-system resources include labor and other funds supporting Air Force IT efforts. If not mapped to an Air Force initiative, the system must indicate the Federal initiative that identifies the resources used for this system in the Federal Budget provided to OMB per OMB Circular A-11 guidance or the exception budget identification number associated with resources that are generally exempted from IT reporting per DoD Financial Management Regulation, Volume 2B, Chapter 18.
1.6.3.1. IT initiatives represent only Air Force Total Obligation Authority as mandated by OMB Circular A-11 and DoD 7000.14-R, Volume 2B. All initiatives are placed into one of the three Sub-enterprise portfolios based on mission area domain assignment. Within the IT Portfolio of each sub-enterprise portfolio, the initiative is assigned to the MAJCOM or functional IT portfolio correlated to its funding Organizational Account Code (OAC). Where two or more MAJCOM, Combatant Commands, or HAF functional areas allocate funds, initiatives are assigned to the lead command, agency, or organization.
1.6.3.1.1. Initiatives within the Air Force IT portfolio are categorized into the following types: system, program, project, organization, payment, or family of systems.
1.6.3.1.1.1. System – A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information.
1.6.3.1.1.2. Program – An approved and funded effort.
1.6.3.1.1.3. Project – An IT effort focused on a specific product or result with a more distinct end state.
1.6.3.1.1.4. Organization – Cost of operating an organization whose primary function is IT.
1.6.3.1.1.5. Payment – A payment for IT services, such as payment to DISA.
1.6.4. Given the large amount of the data collection, management, analysis, and reporting requirements associated with IT portfolio management, a single data repository should be used to preclude repetitious entry of identical data into multiple databases while eliminating potential confusion over the primacy of conflicting data. EITDR is the Air Force IT Portfolio Management system of record. EITDR is accessible through the Air Force Portal. EITDR contains a current inventory of initiatives, systems, and

system-related data and is used for internal management and oversight as well as to provide information to external sources to satisfy statutory and regulatory requirements.

1.6.4.1. A subset of the data residing in the EITDR will be uploaded quarterly to the DoD IT Portfolio Repository (DITPR) in compliance with the annual DITPR guidance. This process is used to satisfy several DoD reporting requirements. Accordingly, IT Functional Portfolio Managers are responsible to ensure the currency, completeness and accuracy of all data within their portfolios to preserve the integrity of Air Force reporting.

1.6.4.2. All IT initiative core information, as identified in the EITDR, must be updated at least semiannually in conjunction with semiannual budget cycle data submissions.

1.6.5. IT Registration. All Air Force IT should be registered in the appropriate Air Force and DoD registries.

1.6.5.1. System registration consists of core data, as identified in EITDR. Core data includes, but is not limited to, name, acronym, description, GIG and mission domain alignment. SAF/XCP will coordinate new system registrations with OSD. IT systems shall be registered and their information maintained in the EITDR or an Intelligence Community Registry. To facilitate IT portfolio management, all systems must map to a specific initiative. IT system registration complements the IT portfolio management process and supports other essential Air Force processes.

1.6.5.2. IT initiatives form the framework of the individual MAJCOM, Combatant Command, and HAF functional IT portfolios. IT initiative core information modification, including new submissions, requests for archiving, and requests for transfers between portfolios, must be submitted by the MAJCOM, Combatant Command, DRU, HAF or HAF functional IT Portfolio Management POC to SAF/XCPR. SAF/XCPR will coordinate core initiative information with OSD. OSD must review and approve all initiative requests (additions, modifications, and archivals). Transfers between portfolios must be approved in advance by both IT Portfolio Management POCs.

1.6.6. IT Budget Reporting. The instructions below apply to all IT portfolios. Additional budgetary reporting requirements will be provided within appropriate PPBE guidance, and supplemented with additional guidance documents as necessary through the budget cycle.

1.6.6.1. Budget submissions include two types of information: resource data and business case data. Both sets of data must be updated each budget cycle to reflect the official organizational position at the time of submission.

1.6.6.2. Resource Data. The resource data includes financial data for the entire Future Years Defense Program (FYDP). All initiatives must report this information even if other business case information is not required through the FYDP. Prior budget year funding information is required even if the initiative will not be requesting funding in the budget cycle.

1.6.6.3. Business Cases. Business case data collection during the budget cycle supports multiple internal and external analyses and reporting requirements. At a minimum, business case data elements must meet external source (OMB, Congress, OSD, etc.) data element requirements.

1.6.6.3.1. Capital Investment Report (CIR). CIRs are used by OSD to meet OMB Circular A-11, Exhibit 300, reporting requirements. SAF/XCPRP will oversee the transfer of the required initiative CIRs between the MAJCOM, Combatant Command, DRU, HAF and HAF functional IT portfolios to OSD and OMB. These specific reporting requirements are subject to change annually by the OMB.

1.6.6.3.2. Selected CIR (SCIR). SCIRs are used by OSD to meet PL 108-136, *National Defense Authorization Act* for Fiscal Year 2003, reporting requirements. SAF/XCPRP will oversee the transfer of the required SCIRs between the MAJCOM, Combatant Command, DRU, HAF and HAF functional IT portfolios to OSD and Congress based on the annual request from OSD and Congress. This additional data will be collected and reported via the EITDR as soon as annual reporting requirements are published.

1.6.6.4. Statement of Compliance. During each budget reporting cycle, the MAJCOM, Combatant Command, DRU, HAF and HAF functional IT portfolio managers and corresponding Chief Financial Officers (or equivalent) must provide a Statement of Compliance to the AF CIO. Statement of compliance must be coordinated with the organizational plans and programs directorates and/or directorates of requirements (or equivalent). The statement validates the budget submission is complete, accurately aligned with primary budget, program and/or acquisition materials; and is consistent with the Division E, PL 104-106, OMB Circular A-11, and documented exceptions to the Circular, DoD CIO budget guidance memorandum, and other applicable acts. The statement should also include explanations for initiatives that do not conform. The MAJCOMs statement must be provided before 30 days of closure of the official budget submission. The overall Air Force letter is due within 30 days.

1.6.7. Security. The importance of network security has grown rapidly in recent years and IT systems are subjected to greater scrutiny. IA is no longer the province of technical experts, but now touches everyone who develops or uses IT. The majority of IA data collection and reporting requirements stem from the Federal Information Security Management Act (FISMA). Additional requirements can be found in AFI 33-202, Volume 1, *Network and Computer Security*. A summary of major data collection requirements follows.

1.6.7.1. In accordance with DoDI 8510.01, Defense Information Assurance Certification and Accreditation Process, all IT systems, including stand-alone systems, require a security vulnerability assessment, and all IT systems (to include those with an IT platform interconnection) must have and maintain a Certification and Accreditation (C&A), in accordance with the DoDI 8510.01, to operate on the Air Force enterprise network. Due to the nature of EITDR and the requirements for all systems to be registered in EITDR, we recognize that it has classified and unclassified systems registered in the database. Classified systems are only required to input basic information and complete their process through other means. C&A data is collected in the EITDR and reported annually as part of the FISMA report. Systems without a current C&A (or with an Interim Approval to Operate) are also required to submit a Plan of Action and Milestones (POA&M) for obtaining a C&A (or an Approval to Operate (ATO)). Current POA&M dates are reflected in the EITDR on the PfM side.1.6.7.2. Additional data elements, such as contingency and security control test dates, are collected and reported as part of FISMA. These specific reporting requirements are subject to change annually by the OMB. This additional data will be collected and reported via the EITDR as soon as annual reporting requirements are published.

1.6.8. IT Lean Reengineering in accordance with *AFI 63-101*. The IT Lean process applies to programs in acquisition or sustainment including upgrades or modernizations *(see Information Technology Lean Reengineering CoP for details).* The IT Lean Process uses the EITDR to store, manage, and assess derived Security, Interoperability, Supportability, Sustainability, and Usability (SISSU) information for Air Force IT programs.

1.6.9. Ronald Reagan National Defense Authorization Act (NDAA) Certification. Fiscal Year (FY) 2005 NDAA states that funds appropriated under the DoD may not be obligated for a defense business system modernization that will have a total cost in excess of $1M unless it is certified by the designated approval authority as necessary to achieve a critical national security capability or address a critical requirement in an area such as security or safety; or is necessary to prevent a significant adverse effect on a project that is needed to achieve an essential capability, taking into consideration alternative solutions.

1.6.9.1. SAF/XC is the pre-certification authority (PCA) for Air Force business systems and certifies systems based on recommendation from the Senior Working Group (SWG). OSD Investment Review Boards (IRBs) are the certification authority (CA) for defense business systems.

1.6.9.2. The NDAA Certification process includes the certification review and the annual review. SAF/XCP is the lead for NDAA Certification and is responsible for distributing guidance and suspense dates. Air Force IT Investment Review guide and reference materials, providing detail instructions on the Air Force certification and annual review processes, are located in the AF IT Investment Compliance Review Community of Practice (COP) accessible from the Air Force Portal.

1.6.10. Others Processes. Other individuals or organizations may provide action and/or information as needed to facilitate the IT portfolio management process.

1.6.11. IT Compliance Process.

1.6.11.1. CCA Compliance. Any space program, non-space program or business system must be in compliance with the requirements of the Clinger-Cohen Act (CCA) as amended by Public Law 104-106 and DoDI 5000.2. Confirmation of compliance can be provided by DoD CIO, AF CIO, or SAF/XCP.

1.6.11.2. Privacy. The Privacy Act of 1974 As Amended places the responsibility on the U.S. Government to inform the public that a Privacy Act system of records is being established. The eGovernment Act of 2002 requires the U.S. Government to assess how the public's Personally Identifiable Information (PII) is being protected in an IT system/service. OMB Memorandum M-07-16, released May 22, 2007, encourages Federal agencies to reduce the use of personally identifiable information, especially Social Security Numbers.

1.6.11.3. Section 508 Compliance. PL 105-220, Section 508 of the Rehabilitation Act as amended requires that Federal departments and agencies developing, procuring, maintaining, or using Electronic and Information Technology (E&IT) ensures that Federal employees and members of the public with disabilities have access to and use of information and data, comparable to that of Federal employees and members of the public without disabilities.

1.6.11.4 DoD and Air Force Enterprise Architect Compliance. DoD and Air Force architectures capture information reflecting the organizations' current state, desired future state, transition strategy, and implementation guidance and standards necessary to ensure that all IT/NSS capabilities are implemented in such a way to enable the desired future state. Both federal and DoD guidance require the use of architecture to guide IT/NSS modernization. As a result, all IT National Security System (NDAA) must conform to the standards and guidance reflected in published DoD and Air Force architectures. Both DoD and Air Force will publish architecture compliance criteria which will be used to assess whether IT/NSS systems are being implemented correctly. The evidence that IT/NSS systems provide to support their assertions of compliance will, in turn, be used to support operational and technical testing of the systems. Additional requirements can be found in AFI 33-401, Implementing Air Force Architectures.

1.6.11.5. EITDR is the database for ensuring compliance and serves as the official record for monitoring compliance with other standing and ad hoc requirements.

Chapter 2

AF IT INVESTMENT REVIEW

2.1 Background. The DoD Mission Areas (MAs) provide life cycle oversight to applicable DoD Component and Combatant Commander IT investments (systems or initiative/systems – IT and/or National Security System (NSS)). IT Lean is required for all IT investments less than $15 million. MA IT systems investments support and enhance the Chairman of the Joint Chiefs of Staff's joint warfighting priorities. They also support actions to create a net-centric distributed force, capable of full spectrum dominance through decision and information superiority.

2.2. Ronald Reagan National Defense Authorization Act (NDAA) Certification Requirement. The FY 2005 NDAA established the Defense Business Systems Management Committee (DBSMC) and the Approval Authority (AA) structure. Starting 1 October 2005, program managers must obtain DBSMC-approved certification prior to obligating funds on a defense business system modernization that has a total system modernization cost in excess of $1M, for all appropriations including operations and maintenance (O&M) through the FYDP. For O&M, only those funds used to modernize the system should be included. Those used to operate and sustain the system should not be included. Per the FY05 NDAA, failure to obtain DBSMC approval may result in an Anti-Deficiency Act violation. Air Force implementation of the NDAA certification and annual review processes are documented in the Air Force IT Investment Review Guide.

2.3. Portfolio Investment Review. Per DoDI 8115.02, the DoD IT Portfolio management process continues the evolution from an emphasis on individual systems to overall mission capability. Consistent with the Office of Management and Budget (OMB) Capital Planning and Investment Control guidance, the Air Force will use four continuous integrated activities to manage its portfolios - analysis, selection, control, and evaluation. The overall process is iterative, with results being fed back into the process to guide future decisions. Air Force implementation of the portfolio investment process is documented in the Air Force IT Investment Review Guide.

2.4. Information Collections, Records, and Forms.
2.4.1. Information Collections. No information collections are created by this publication.
2.4.2. Records. No records are created by this publication.
2.4.3. Forms (Adopted and Prescribed).
2.4.3.1. Adopted Forms: AF Form 847, **Recommendation for Change of Publication**.
2.4.3.2. Prescribed Forms: No forms are prescribed by this publication.

MICHAEL W. PETERSON, Lt Gen, USAF
Chief of Warfighting Integration and
Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Title 40, U.S.C., Sections 11101-11704, *Information Technology Management* (40 U.S.C. 11101-11704) (*Clinger-Cohen Act of 1996 (CCA)*)
PL 108-136, *National Defense Authorization Act*
CJCSI 3170.01E, *Joint Capabilities Integration and Development System*
CJCSI 6212.01C, *Interoperability and Supportability of Information Technology and National Security Systems*
CJCSI 8410.01, *Warfighting Mission Area Information Technology Portfolio Management and Net-Centric Data Sharing*
DoDD 4630.5, *Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*
DoDD 5000.1, *The Defense Acquisition System*
DoDD 8500.1, *Information Assurance (IA)*
DoDD 8115.01, *Information Technology Portfolio Management*
DoDI 8115.02, *Information Technology Portfolio Management Implementation*
DoD 7000.14-R, Volume 2B, *Department of Defense Financial Management Regulations (FMRS)*
DoD 8510.01p, DoD guidance on Information Assurance
DoDI 8510.01 *DIACAP*
DoD Architecture Framework, latest revision
OMB Circular A-11, *Preparation, Submission and Execution of the Budget*
OMB Circular A-130, *Management of Federal Information Resources*
AFDD 2-4, *Combat Support*
AFPD 33-1, *Information Resources Management*
AFPD 33-3, *Information Management*
AFPD 33-4, *Enterprise Architecture*
AFI 10-601, *Capabilities Based Requirements Development*
AFI 33-103, *Requirements Development and Processing*
AFI 33-202, Volume 1, *Network and Computer Security*
AFI 63-101, *Operations of Capabilities Based Acquisition System*
AFI 63-1101, *Modification Management*
AFMAN 33-363, *Management of Records*
AFRIMS RDS, https://afrims.amc.af.mil/rds/index.cfm

Abbreviations and Acronyms

ACS—Agile Combat Support
AF—Air Force
AF CIO—Air Force Chief Information Officer
AFDD—Air Force Doctrine Document
AFI—Air Force Instruction
AFMAN—Air Force Manual
AFPD—Air Force Policy Directive

AFRIMS—Air Force Records Information Management System

AIS—Automated Information System

AO—Action Officer

ATO—Authority to Operate

BMA—Business Mission Area

BTA—Business Transformation Agency

C&A—Certification and Accreditation

CBM—Core Business Mission

CCA—The Clinger-Cohen Act of 1996

CIO—Chief Information Officer

CIR—Capital Investment Report

CoP— Community of Practice (AF IT Investment Compliance Review)

DAA—Designated Approval Authority

DAS—Defense Acquisition System

DBSMC—Defense Business Systems Management Committee

DITPR—DoD Information Technology Portfolio Repository

DoD—Department of Defense

DoDD—Department of Defense directive

DoDI—Department of Defense Instruction

DRU—Direct Reporting Unit

EA—Enterprise Architecture

EIE—Enterprise Information Environment

EIEMA—Enterprise Information Environment Mission Area

EITDR—Enterprise Information Technology Data Repository

ETP—Enterprise Transition Plan

FISMA—Federal Information Security Management Act

FMR- Financial Management Regulation

FOA—Field Operating Agency

FPfM—Functional Portfolio Manager

FY—Fiscal Year

FYDP—Future Years Defense Program

GIG—Global Information Grid

HAF—Headquarters Air Force

HQ AFCA—Headquarters Air Force Communications Agency

HQ USAF—Headquarters United States Air Force

IA—Information Assurance

IRB—Investment Review Board

IS—Information System

IT—information technology

JCIDS—Joint Capabilities Integration and Development System

MAIS—Major Automated Information System

MAJCOM—Major Command

MDAP—Major Defense Acquisition Program

NDAA—National Defense Authorization Act

NSS—National Security System

O&M—Operations and Maintenance

OMB—Office of Management and Budget

OPR—Office of Primary Responsibility

OSD—Office of the Secretary of Defense

PCA—Pre-Certification Authority

PfM—Portfolio Management/Portfolio Manager

PL—Public Law

POA&M—Plan of Action and Milestones

POC—Point of Contact

PPBE—Planning, Programming, Budgeting, and Execution

RDS—Records Disposition Schedule

SAF—Secretary of the Air Force

SCIR—Selected CIR

SECAF—Secretary of the Air Force

SISSU—Security, Interoperability, Supportability, Sustainability, Usability

SME—Subject Matter Expert

SWG—Senior Working Group

U.S.C.—United States Code

WMA—Warfighting Mission Area

Terms

Accreditation - Formal declaration by a Designated Approval Authority (DAA) that an information system is approved to operate in a particular security mode at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. Source: AFI 33-202V1.

Air Force IT Resources - All Air Forces resources (financial, manpower, hardware, software, etc.) used for the development, acquisition, operation, maintenance, sustainment, or modification of IT.

Application - A software program that performs a specific function directly for a user and can be executed without access to system control, monitoring or administrative privileges. Source: DoDD 8500.1.

Architecture - The structure of components, their relationships and the principles and guidelines governing their design and evolution over time. Source: DoDD 4630.5.

Automated Information System (AIS) Application - For DoD information assurance purposes, an AIS application is the product or deliverable of an acquisition program, such as those described in Department of Defense Directive (DoDD) 5000.1, *The Defense Acquisition System,* May 12, 2003. An AIS application performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition. An AIS application may be a single software application; multiple software applications that are related to a single mission; or a combination of software and hardware performing a specific support function across a range of missions. AIS applications are deployed to enclaves for operations, and have their operational security needs assumed by the enclave. Note that an AIS application is analogous to a “major application” as defined in OMB Circular A-130, *Management of Federal Information Resources, Transmittal 4,* November 30, 2000; however, this term is not used in order to avoid confusion with the DoD acquisition category of Major Automated Information System (MAIS). Source: DoDD 8500.1.

Business Mission Area—BMA's objective is to ensure the right capabilities, resources and materiel are reliably delivered to our warfighters: what they need, where they need it, when they need it, anywhere in the world. In order to cost-effectively meet these requirements, DoD's current business and financial management infrastructure – processes, systems, and data standards – are being transformed to ensure better support to the warfighter and improve accountability to the taxpayer. Integration of business transformation for the DoD business enterprise is led by the Deputy Secretary of Defense in his role as Chief Operating Officer of the DoD. The Focused Logistics domain owner works closely with the BMA IRBs. (DoDI 8115.02, Information Technology Portfolio Management (PfM) Implementation)

Certification - Comprehensive evaluation of the technical and non-technical security features and countermeasures of an information system to establish the extent to which a particular design and implementation meet a set of specified security requirements. Source: AFI 33-202V1.

Defense Business System—'Defense Business System' means an information system, other than a national security system, operated by, for, or on behalf of the Department of Defense, including financial systems, mixed systems, financial data feeder systems, and information technology and information assurance infrastructure, used to support business activities, such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management. (FY2005 NDAA)

Defense Business System Development/Modernization (Dev/Mod)—Also referred to as development/modernization/enhancement. Any change or modification to an existing Information System (IS), program, and/or initiative that results in improved capability or performance of the baseline activity. Improved capability or performance achieved as a by-product of the replacement of broken IT equipment to continue an operation at the current service levels is not categorized as Development/Modernization. Development/Modernization includes: (1) program costs for new applications and infrastructure capabilities that are planned or under development; (2) any change or modification to existing applications and infrastructure capabilities which is intended to result in improved capability or performance of the activity. These changes include (a) all modifications to existing operational software (other than corrective software maintenance); and (b) expansion of existing capabilities to new users; (3) changes mandated by Congress or the Office of the Secretary of Defense; (4) personnel costs for Project Management. (DoD Financial Management Regulation, Chapter 18)

Enclave - A collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves are analogous to general support systems as defined in OMB Circular A-130, *Management of Federal Information Resources, Transmittal 4*, November 30, 2000. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers. Source: DoDD 8500.1.

Enterprise Information Environment Mission Area—EIEMA represents common, integrated information computing and communications environment of the Global Information Grid (GIG). The Enterprise Information Environment (EIE) is composed of GIG assets that operate as, provide transport for and/or assure local area networks, campus area networks, tactical, operational and strategic networks, metropolitan area networks, and wide area networks. EIE includes computing infrastructure for the automatic acquisition, storage, manipulation, management, control, and display of data or information, with a primary emphasis on DoD enterprise hardware, software operating systems, and hardware/software support that enable the GIG enterprise. The EIE also includes a common set of enterprise services, called Core Enterprise Services, which provide awareness of, access to, and delivery of information on the GIG. The Net-centric and Command and Control domain owners work closely with the EIEMA IRBs. (DoDI 8115.02, Information Technology Portfolio Management Implementation)

Family of Systems - A set or arrangement of independent systems that can be arranged or interconnected in various ways to provide different capabilities. Source: DoD Architecture Framework, Version 1

Information Assurance (IA) - Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Source: DoDD 8500.1.

Information System (IS)—A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (DoDD 8000.1, Management of DoD Information Resources and Information Technology). Or a discrete set of information resources organized for collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. (Note: Includes automated information system (AIS) applications, enclaves, outsourced IT-based processes, and platform IT interconnections.) (DoDD 8500.01)

Information Technology (IT)—Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes equipment used by the executive agency directly or used by a contractor under a contract with the executive agency, which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term “IT” includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. Notwithstanding the preceding, the term "IT” does not include any equipment that is required by a federal contractor incident to a federal contract. The term “IT” includes National Security Systems (NSS), and is synonymous with the term "information system" (IS). (DoDD 4630.5, DoDD 8000.1, 40 U.S.C. 11101(6))

Initiative - A collection of resources focused on a single IT project. Initiatives include both new starts and ongoing efforts, and that a single initiative, in the IT 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 IT

IT Investment—The development and sustainment resources needed in support of IT or IT-related initiatives. 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 (DoDD 8115.01, Information Technology Portfolio Management). WMA IT investments recommendations will focus on whether acquisition programs, IT systems, and budget initiatives should be initiated, modified, continued, or terminated. Specific financial and/or budget information will support program, system, and initiative recommendations. (CJCSI 8410.01, Warfighting Mission Area Information Technology Portfolio Management and Net-Centric Data Sharing)

IT Portfolio - A grouping of IT initiatives by capability to accomplish a specific functional goal, objective, or mission outcome. Source: DoDD 8115.01

IT Portfolio Management (Portfolio management) - The management of selected groupings of IT resources using strategic planning, architectures, and outcome-based performance measures to achieve a mission capability (CJCSI 8410.01, Warfighting Mission Area Information Technology Portfolio Management and Net-Centric Data Sharing). Source: DoDD 8115.01

Mission Area—A defined area of responsibility with functions and processes that contribute to mission accomplishment. (CJCSI 8410.01, Warfighting Mission Area Information Technology Portfolio Management and Net-Centric Data Sharing)

National Security System (NSS) - Any telecommunications or information system operated by the United States 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 weapons system, or is critical to the direct fulfillment of military or intelligence missions. Such a system is not NSS if it is to be used for routine administrative and business applications (including payroll, finance, logistics and personnel management applications). Source: CJCSI 6212.01C

SISSU Checklist - A consolidated list of SISSU requirements (i.e., non-functional requirements) that is used to guide the requirements sponsor and program manager through the process to ensure that all SISSU needs are met when developing and fielding a system. The SISSU Checklist is a tool that stakeholders use to ensure that SISSU needs are communicated early, from requirements generation forward. The SISSU Checklist specifies in which phase in the IT Lean Process (i.e., define need, design, build and test, and release and support) the requirements must be fulfilled. Source: *AFI 63-101*.

Warfighting Mission Area—WMA is one of four DoD IT mission areas contributing to DoD IT (to include NSS) investment management. WMA includes eight IT Domains that will provide oversight to applicable DoD component and Combatant Commander IT Programs. WMA IT investments (programs, systems, and initiatives) support and enhance the Chairman's joint warfighting abilities while supporting actions to create a net-centric distributed force, capable of full spectrum dominance through decision and information superiority. WMA IT investments ensure Combatant Commands can meet the Chairman's strategic challenges to win the war on terrorism; accelerate transformation; and strengthen joint warfighting. WMA IT investments provide organizational agility, action and decision speed, collaboration and outreach. (CJCSI 8410.01, Warfighting Mission Area Information Technology Portfolio Management and Net-Centric Data Sharing)

WMA IT Domain—Subset of the warfighting mission area representing a common collection of related, or highly dependent, information capabilities and services. Managing these related information capabilities and services within domains improves coordination, collaboration, integration, and consistency of processes and interfaces for information sharing. IT Domains are the basic organization established in WMA to conduct IT Portfolio Management and COI oversight. WMA IT Domains are aligned to the JCIDS FCBs. (CJCSI 8410.01, Warfighting Mission Area Information Technology Portfolio Management and Net-Centric Data Sharing)

Attachment 2

AIR FORCE INFORMATION TECHNOLOGY (IT) PORTFOLIO OWNER LIST

Air Combat Command (ACC)
Air Education and Training Command (AETC)
Air Force Materiel Command (AFMC)
Air Force Reserve Command (AFRC)
Air Force Space Command (AFSPC)
Air Force Special Operations Command (AFSOC)
Air Force Operational Test and Evaluation Center (AFOTEC)
Air Force District of Washington (AFDW)
Air Mobility Command (AMC)
Air National Guard (ANG)
Air Force Surgeon General (HQ USAF/SG)
Deputy Chief of Staff, Information, Surveillance, and Reconnaissance (HQ USAF/A2)
Deputy Chief of Staff, Air and Space Operations (HQ USAF/A3)
Deputy Chief of Staff, Installations and Logistics (HQ USAF/A4)
Deputy Chief of Staff, Personnel (HQ USAF/A1)
Deputy Chief of Staff, Plans and Programs (HQ USAF/A8)
Deputy Chief of Staff, Studies & Analyses, Assessments and Lessons Learned (HQ USAF/A9)
Director, Information Management for Headquarters Air Force and Headquarters Air Force Chief Information Officer (HAF/IM)
Pacific Air Forces (PACAF)
Secretary of the Air Force, Acquisition (SAF/AQ)
Secretary of the Air Force, Financial Management & Comptroller (SAF/FM)
Secretary of the Air Force, Warfighting Integration and Chief Information Officer (SAF/XC)
United States Air Force Academy (USAFA)
United States Air Forces in Europe (USAFE)
United States Air Force Cyber Command (USAFCYBER)
U.S. Central Command (CENTCOM)
U.S. Northern Command (NORTHCOM)
U.S. Joint Forces Command (JFCOM)
U.S. Special Operations Command (SOCOM)
U.S. Strategic Command (STRATCOM)
U.S. Transportation Command (TRANSCOM)