Form 1221-2
(June 1969)

UNITED STATES
DEPARTMENT OF THE INTERIOR
BUREAU OF LAND MANAGEMENT

Release:1-1784

Date:
12/29/2016

MANUAL TRANSMITTAL SHEET

Subject

H-1265-1 – Capital Planning and Investment Control (CPIC) Handbook [PUBLIC]

1. Explanation of Materials Transmitted: This release transmits Information Technology Investment Management (ITIM) policy as a new Handbook Section. This Handbook provides policy direction for conducting Capital Planning and Investment Control (CPIC) activities for the Bureau of Land Management's IT investments. CPIC is the process the BLM uses for managing internal IT investment portfolios.

2. Reports Required: None

3. Material Superseded: CPIC Handbook dated 8/27/2009, Release 1-1719

4. Filing Instructions: File as directed below

REMOVE	INSERT
All of Release 1-1719	Handbook 1265-1 (Total 88 Sheets)

Janine Velasco
Assistant Director
Business, Fiscal and Information
Resources Management

Department of the Interior
Bureau of Land Management

Information Technology
Capital Planning and Investment Control
Handbook

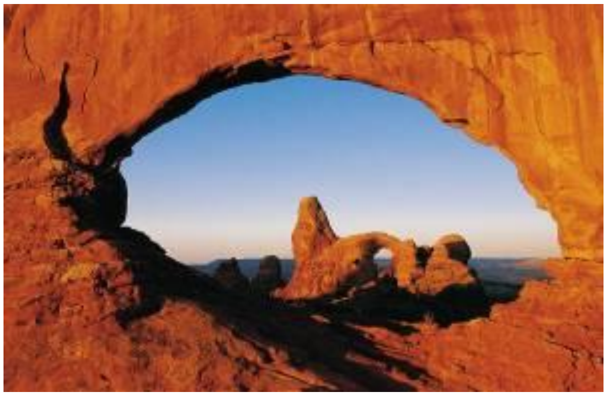


Table of Contents

1 Introduction

1.1 Purpose

This document describes the Bureau of Land Management's (BLM) Information Technology (IT) Capital Planning and Investment Control (CPIC) process. It outlines a framework for managing the BLM IT investment portfolio. The CPIC process enables the BLM to address strategic needs, optimize the allocation of limited IT resources, and comply with applicable regulations and guidance. The Office of Management and Budget (OMB) Circular A-11 "Preparation, Submission and Execution of the Budget" defines CPIC as follows:
"Capital Planning and Investment Control means the same as capital programming and is a decision-making process for ensuring IT investments integrate strategic planning, budgeting, procurement, and the management of IT in support of Agency missions and business needs."

CPIC is a structured, integrated approach for managing IT investments. It ensures that all IT investments align with the BLM mission and support business needs while minimizing risks and maximizing returns throughout the investment's lifecycle. It relies on a systematic process of pre-selection, selection, control, and on-going evaluation ensuring each investment's objectives support the business and mission needs of the BLM.

1.2 Legislative Background & Associated Guidance

Federal Agencies, by statute, are required to continually evaluate their organization and revise their operational and management practices to achieve greater mission efficiency and effectiveness. Some of the key legislation in effect includes:

Clinger-Cohen Act of 1996 (CCA)
Also known as the Information Technology Management Reform Act (ITMRA), the CCA emphasizes an integrated framework of technology aimed at efficiently performing the business of Federal Agencies. Additionally, the CCA provides specific direction to Agencies in the review and approval of their IT investments. It also establishes the role of Chief Information Officer (CIO) as responsible for developing, maintaining, and facilitating the implementation of an integrated IT architecture.

Chief Financial Officers Act of 1990 (CFO Act)
The CFO Act establishes a leadership structure, provides for long-range planning, requires audited financial statements, and strengthens accountability reporting. The CFO Act impacts Federal financial managers at all levels of Government.

Government Performance and Results Act of 1993 (GPRA)

The GPRA provides for the establishment of strategic planning and performance measurement in the Federal Government. The purpose of the GPRA is to improve the effectiveness and accountability of Federal programs by focusing on program results, quality, and customer satisfaction.

Federal Acquisition Streamlining Act of 1994 (FASA)
The FASA simplifies and streamlines the Federal procurement process by reducing paperwork, facilitating the acquisition of commercial products, enhancing the use of simplified procedures for small purchases, transforming the acquisition process to electronic commerce, and improving the efficiency of the laws governing the procurement of goods and services.

Paperwork Reduction Act of 1995 (PRA)
The PRA requires Agencies to plan for the development of new collections of information and the extension of ongoing collections well in advance of sending proposals to OMB. The PRA requires Agencies to seek public comment on proposed collections, certify to OMB that efforts have been made to reduce the burden of the collection, and have in place a process for independent review of information collection requests prior to submission to OMB.

Government Paperwork Elimination Act of 1998 (GPEA)
The GPEA requires Federal Agencies to allow individuals or entities that deal with the Agencies the option to submit information or transact with the Agency electronically, when practicable, and to maintain records electronically, when practicable. The GPEA specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form; and it encourages the Federal Government to use a range of electronic signature alternatives.

Federal Information Security Management Act of 2002 (FISMA)
The FISMA requires that each Federal Agency shall develop, document, and implement an Agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the Agency.

E-Gov Act of 2002
The E-Gov Act requires all Executive Branch Agencies to conduct a privacy impact assessment before developing or procuring IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public or initiating, consistent with the PRA a new electronic collection of information in identifiable form for 10 or more persons.

Federal Information Technology Acquisition Reform Act of 2014 (FITARA)
The FITARA Act of 2014 modified the framework governing the management of IT within the Federal government to require presidential appointment or designation of the CIO in 16 specified federal agencies, designate the Chief Information Officers Council as the lead interagency forum for improving agency coordination information resources investment, and require the Comptroller General to examine the effectiveness of the Council. The FITARA outlines specific requirements related to the Agency CIO authority Enhancements, enhanced transparency and improved risk management in IT Investments, portfolio review, Federal Data Center Consolidation Initiative (FDCCI), expansion of training and use of IT Cadres, maximizing the benefit of the Federal Strategic Sourcing Initiative, and Government wide Software Purchasing Program.

This CPIC Handbook serves as an update to the current direction and processes in place at the BLM and is based on the most recent Department of the Interior (DOI) and OMB guidance[1].

[1] A list of Investment Management reference guides and memoranda is provided in Appendix C of this Handbook

1.3 Point of Contact

Responsibility to oversee the CPIC process falls within the organizational purview of the BLM's Assistant Director (AD) of Business, Fiscal and Information Resources Management (BFIRM). For further information about this Handbook or the CPIC process, contact the Chief, Division of Investment Management (InvM).

1.4 Scope of CPIC

All BLM investments expended upon IT based goods and services must comply with the policy mandates of this Handbook.

1.5 Roles and Responsibilities

1.5.1 Decision Making Body, Support Staff, Offices, and Personnel

The Information Technology Investment Board (ITIB): The ITIB is responsible for building an IT investment foundation, and developing and maintaining a complete IT investment portfolio. The ITIB is the decision making board for all IT investments. In executing its responsibilities, the Board adopts and enforces policies, processes and procedures to ensure current and future IT investment successes are realized. The ITIB plans for and manages information systems and IT in concert with other planning and management processes. The ITIB establishes, maintains and documents policies and processes for IT planning and governance; conducting strategic information systems and technology planning; data management; Enterprise Architecture (EA) planning and management; and IT Portfolio Management and CPIC. The ITIB implements IT Investment and Portfolio planning, management, and reporting. The ITIB provides oversight to Budget Planning, Workforce Planning, Asset Tracking and Data Management. Membership to the ITIB consists of the BLM Deputy Director of Operations, State Directors (SDs), Center Directors (CD), ADs of Washington Office (WO), Field Committee (FC) Representative, and BMC Representative.[2]

The BLM's AD-BFIRM: The BLM's AD-BFIRM is responsible for coordinating all development and overall management of IT investments and assets for the BLM. The AD-BFIRM also oversees the BLM's compliance with Federal and Departmental policies, guidelines, and regulations governing the management of these investments and assets.

The Executive Leadership Team (ELT): Membership to the ELT consists of the BLM Director, BLM Deputy Director, SDs, CDs, and ADs.

The Field Committee (FC): The BLM's FC serves as a senior leadership forum for the operational decision makers to assure the uniform implementation of the BLM operations and the BLM Strategic Plan;

[2] Appendix C-1

to act as a BLM sounding board for national and state policy matters, as well as provide insight and advice on sensitive issues; to develop, share and exchange best practices to improve operational efficiency; to advise and make recommendations to foster mentoring, training, and leadership development; and to serve as a nexus between field operations and the ELT. Membership to the FC consists of the BLM Deputy Director of Operations, Associate State Directors, Deputy ADs of WO, Associate National Operations Center (NOC) Director, and Deputy Director, Office of Fire and Aviation.[3]

The Business Management Council (BMC): The BLM's BMC is responsible for administering the business and support functions of the BLM. The purpose of the BMC is to strategically set goals, standards, and make recommendations to guide future BLM business and support functions; to cooperatively resolve current issues of major significance that will impact the business and support programs of the BLM; to develop consistent frameworks to enhance the implementation of business and support programs among competing priorities while maintaining flexibility for using best practices; to exchange information for program development and skills building; and to foster trust and consensus among the BMC and internal partners. Membership to the BMC consists of the Deputy State Directors (DSDs) for Support Services (or Business Resources); Division Chief, Support Services, National Interagency Fire Center; Director of the National Training Center; and Director of the NOC.[4]

The Geospatial Steering Committee (GSC): The BLM's GSC is responsible for providing strategic direction and oversight to the Geospatial program for the BLM. The focus of the GSC is on providing strategic direction and oversight for the ELT's vision of One GIS, setting priorities for the Geospatial program, and providing executive level coordination. Membership to the GSC consists of the ADs of WO; SDs, Director of the NOC and the Senior Geospatial Program Manager.[5]

Rating and Ranking Committee (RRC): The role of the RRC is to review and assess the health of all BLM IT Investments, and to make recommendations for further improvement. The RRC will rate and rank the BLM IT Investments in accordance with the rating and ranking criteria established by the ITIB. Membership to the RRC is determined by the ITIB.

Division of Investment Management Washington Office-860 (WO-860): The Investment Management Division is responsible for planning, budgeting, acquisition, compliance and oversight of the BLM IT capital assets. The role of the InvM is to ensure that the BLM is maximizing the value and highest use of IT funds; achieve strategic performance goals and objectives of the BLM investment portfolio at the lowest life-cycle costs and least risk; provide oversight of the BLM capital plan and business case and the IT investment portfolio; ensure policy oversight and monitor compliance for the national acquisition of IT contractual goods and services; and support the ITIB.

States, Centers, and Directorates: Are responsible for selecting, controlling, and evaluating all IT investments unique to their Offices and are within the threshold and criteria defined in Section 1.7 of the Handbook. States, Centers, and Directorates are not required to have individual ITIBs. However, each office is required to review IT investments through a documented process, utilize decision criteria, document deliberations, track outcomes, and evaluate results. This information should be made available to the Investment Management team as they are required to report portions of it to the DOI and the OMB. The States, Centers, and Directorates are responsible for ensuring that the CPIC process objectives are carried out within their areas of responsibility and ensuring that skilled PMs are assigned

[3] Appendix C-2
[4] Appendix C-3
[5] Appendix C-4

to oversee and manage all IT systems and software under their jurisdiction.

Investment Sponsor or System Owner or Business Manager (BM): The business official responsible for the strategic business processes under development or enhancement and for ensuring their integrity; also serves as the primary user interface to the CIO and the ITIB. The Investment Sponsor is responsible for securing funding for the investment once it is approved by the ITIB. The Investment Sponsor is also responsible for ensuring that the system is evaluated annually and receives an appropriate level of funding for the Operations and Maintenance (O&M) of the system.

Project Manager (PM): The trained or experienced official responsible for management and completion of one or more IT investment projects. The PM is assigned the responsibility for accomplishing a specifically designated work effort or group of closely related efforts established to achieve stated or designated objectives, defined tasks, or other units of related effort on a schedule, within cost constraints and in support of the program mission or objective. The PM is responsible for the planning, controlling, and reporting of the project, and for the management of required functions, including acquisition planning, developing the requirements, business case development, performance of the schedule, and formulation, justification and execution of the budget. The PM is responsible for effectively managing project risks to insure effective systems and services are delivered through a total life-cycle approach to the end user on schedule, within budget and at the required levels of performance. PMs assigned to Major Investments must be senior-level certified Federal Acquisition Certification for Program and Project Managers (FAC-P/PM). Other PMs must be, at a minimum, mid-level certified FAC-P/PM.[6]

1.5.2 Relationship

Figure 1-1 provides a summary of the relationship between the ITIB and other committees and organizations within BLM.

[6] Appendix C-6

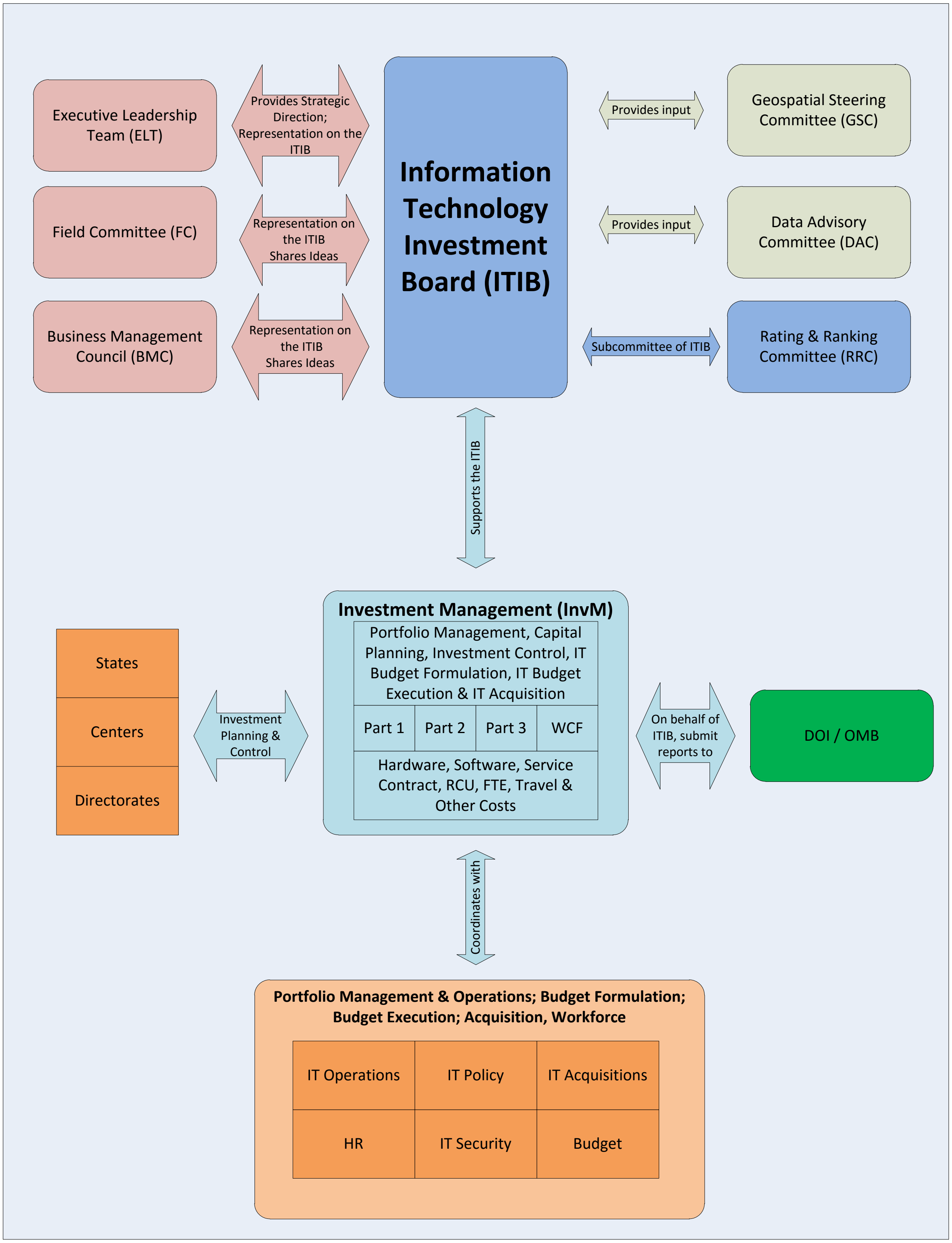

Executive Leadership Team (ELT)
Provides Strategic Direction; Representation on the ITIB
Field Committee (FC)
Representation on the ITIB Shares Ideas
Business Management Council (BMC)
Representation on the ITIB Shares Ideas
Information Technology Investment Board (ITIB)
Provides input
Geospatial Steering Committee (GSC)
Provides input
Data Advisory Committee (DAC)
Subcommittee of ITIB
Rating & Ranking Committee (RRC)
Supports the ITIB
Investment Management (InvM)
Portfolio Management, Capital Planning, Investment Control, IT Budget Formulation, IT Budget Execution & IT Acquisition
Part 1
Part 2
Part 3
WCF
Hardware, Software, Service Contract, RCU, FTE, Travel & Other Costs
States
Centers
Directorates
Investment Planning & Control
On behalf of ITIB, submit reports to
DOI / OMB
Coordinates with
Portfolio Management & Operations; Budget Formulation; Budget Execution; Acquisition, Workforce
IT Operations
IT Policy
IT Acquisitions
HR
IT Security
Budget

Figure 1-1: Relationship

1.6 CPIC and OMB Circular A-130

The OMB revised the Circular A-130 "Managing Information as a Strategic Resource" in July 2016. The Circular A-130 establishes general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, IT resources and supporting infrastructure and services. The requirements of the Circular A-130 apply to the information resources management activities of all agencies of the Executive Branch of the Federal Government. The Circular A-130 sections pertinent to performing CPIC activities are provided below.

The Circular A-130's Section 4 "Basic Considerations" explains that Federal information is both a strategic asset and a valuable national resource. It enables the Government to carry out its mission and programs effectively. It provides the public with knowledge of the Government, society, economy, and environment – past, present, and future. Federal information is also a means to ensure the accountability of Government, to manage the Government's operations, and to maintain and enhance the performance of the economy, the public health, and welfare. Appropriate access to Federal information significantly enhances the value of the information and the return on the Nation's investment in its creation. The following considerations reflect these principles:

a. The free flow of information between the Government and the public is essential to a democratic society. Therefore, the management of Federal information resources shall protect the public's right of access to Federal information;
b. Government agencies shall be open, transparent, and accountable to the public. Promoting openness and interoperability, subject to applicable legal and policy requirements, increases operational efficiencies, reduces costs, improves services, supports mission needs, and increases public access to valuable Federal information;
c. Making Federal information discoverable, accessible, and usable can fuel entrepreneurship, innovation, and scientific discovery that improves the lives of Americans, and contributes significantly to national stability and prosperity, and fosters public participation in Government;
d. The Federal Government shall provide members of the public with access to public information on Government websites. This responsibility includes taking affirmative steps to ensure and maximize the quality, objectivity, utility, and integrity of Federal information prior to public dissemination, and maintaining processes for addressing requests for correction of information disseminated publicly;
e. The open and efficient exchange of scientific and technical Federal information, subject to applicable security and privacy controls and the proprietary rights of others, fosters excellence in scientific research and effective use of Federal research and development resources;
f. Federal information is a strategic asset subject to risks that must be managed to minimize harm;
g. Protecting an individual's privacy is of utmost importance. The Federal Government shall consider and protect an individual's privacy throughout the information life cycle;
h. While security and privacy are independent and separate disciplines, they are closely related, and it is essential for agencies to take a coordinated approach to identifying and managing security and privacy risks and complying with applicable requirements;
i. The design of information collections shall be consistent with the intended use of the information, and the need for new information shall be balanced against the burden imposed on the public, the cost of the collection, and any privacy risks;

j. It is essential that the Federal Government minimize the Federal information collection burden on the public, minimize the costs of its information activities, and maximize the usefulness of Government information; and
k. Attention to the management of Federal Government records from creation to disposition is an essential component of sound information resources management that promotes public accountability. Together with records preservation, it helps protect the Federal Government's historical record and safeguards the legal and financial rights of the Federal Government and the public.

The Circular A-130's Section 5 "Policy" requires agencies to establish a comprehensive approach to improve the acquisition and management of their information resources by: performing information resources management activities in an efficient, effective, economical, secure, and privacy-enhancing manner; focusing information resources planning to support their missions; implementing an IT investment management process that links to and supports budget formulation and execution; and rethinking and restructuring the way work is performed before investing in new information systems.

The Circular A-130's Section 5.d "Policy, IT Investment Management" requires the policies described in the following sub-sections be implemented with regards to CPIC.

1.6.1 A-130 5.d.1 Acquisition of Information Technology and Services

Agencies shall:

a. Make use of adequate competition, analyze risks (including supply chain risks) associated with potential contractors and the products and services they provide, and allocate risk responsibility between Government and contractor when acquiring IT;
b. Conduct definitive technical, cost, and risk analyses of alternative design implementations, including consideration of the full life cycle costs of IT products and services, including but not limited to, planning, analysis, design, implementation, sustainment, maintenance, re-competition, and retraining costs, scaled to the size and complexity of individual requirements;
c. Consider existing Federal contract solutions or shared services when developing planned information systems, available within the same agency, from other agencies, or from the private sector to meet agency needs to avoid duplicative IT investments;
d. Acquire IT products and services in accordance with Government-wide requirements;
e. Ensure that decisions to improve existing information systems with custom-developed solutions or develop new information systems are initiated only when no existing alternative private sector or governmental source can efficiently meet the need, taking into account long-term sustainment and maintenance;
f. Structure acquisitions for major IT investments into useful segments, with a narrow scope and brief duration, in order to reduce risk, promote flexibility and interoperability, increase accountability, and better match mission need with current technology and market conditions;
g. To the extent practicable, modular contracts for IT, including orders for increments or useful segments of work, should be awarded within 180 days after the solicitation is issued. If award cannot be made within 180 days, agencies shall consider cancelling the solicitation. The IT acquired should be delivered within 18 months after the solicitation resulting in award of the contract was issued;
h. Align IT procurement requirements with larger agency strategic goals;
i. Promote innovation in IT procurements, including conducting market research in order to maximize utilization of innovative ideas; and

j. Include security, privacy, accessibility, records management, and other relevant requirements in solicitations.

1.6.2 A-130 5.d.2 Agency Approval

Agencies shall ensure that all acquisition strategies, plans, and requirements (as described in Federal Acquisition Regulation (FAR) Part 7), or interagency agreements (such as those used to support purchases through another agency) that include IT are reviewed and approved by the purchasing agency's CIO. These approvals shall consider the following factors:

a. Alignment with mission and program objectives in coordination with program leadership;
b. Appropriateness with respect to the mission and business objectives supported by the IRM Strategic Plan;
c. Inclusion of innovative solutions;
d. Appropriateness of contract type for IT-related resources;
e. Appropriateness of IT-related portions of statement of needs or statement of work;
f. Ability to deliver functionality in short increments;
g. Inclusion of Government-wide IT requirements, such as information security; and
h. Opportunities to migrate from end-of-life software and systems, and to retire those systems.

1.6.3 A-130 5.d.3 Investment Planning and Control

Agencies are responsible for establishing a decision-making process that shall cover the life of each information system and include explicit criteria for analyzing the projected and actual costs, benefits, and risks, including information security and privacy risks, associated with the IT investments. Agencies shall designate IT investments according to relevant statutes, regulations, and guidance in OMB Circular A-11, and execute processes commensurate with the size, scope, duration, and delivery risk of the investment. The IT investment processes shall encompass planning, budgeting, procurement, management, and assessment. For further guidance related to investment planning, refer to OMB Circular A-11, including the Capital Programming Guide. At a minimum, agencies shall ensure that:

a. All IT resources are included in IT investment planning documents or artifacts;
b. Decisions related to major IT investments are supported by business cases with appropriate evidence;
c. IT investments implement an agile development approach, as appropriate;
d. IT investments support and enable core mission and operational functions and processes related to the agency's missions and business requirements;
e. IT capital investment plans and budgetary requests are reviewed to ensure that Government-wide requirements, as well as any associated costs, are explicitly identified and included, with respect to any IT resources. This includes IT resources that will be used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and
f. Decisions to improve, enhance, or modernize existing IT investments or to develop new IT investments are made only after conducting an alternatives analysis that includes both government-provided (internal, interagency, and intra-agency where applicable) and commercially available options, and the option representing the best value to the Government has been selected.

1.6.4 A-130 5.d.4 Selection Criteria and Requirements

Agencies shall consider the following factors when analyzing IT investments:

a. Qualitative and quantitative research methods are used to determine the goals, needs, and behaviors of current and prospective managers and users of the service to strengthen the understanding of requirements;
b. All decisions concerning the selection of information system technologies and services – including decisions to acquire or develop custom or duplicative solutions – shall be merit-based and consider factors such as, but not limited to, ability to meet operational or mission requirements, total life cycle cost of ownership, performance, security, interoperability, privacy, accessibility, ability to share or reuse, resources required to switch vendors, and availability of quality support. Consistent with the FAR, contracts for custom software development are to include contractual provisions that reaffirm the right to reuse the software throughout the Federal Government;
c. Agencies shall consider use of suitable existing Federal information technology resources and commercially-available solutions in order to ensure effective management of Federal resources. Consistent with law and regulation, agencies should consider and evaluate the suitability of existing Federal information technologies and related services, including software, Federal shared services, and commercially-available solutions before embarking upon new developments of software and information technologies; and
d. Information systems security levels are commensurate with the impact that may result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information consistent with NIST standards and guidelines.

1.6.5 A-130 5.d.5 IT Investment Design and Management

Agencies shall implement the following requirements:

a. Information systems and processes must support and maximize interoperability and access to information, where appropriate, by using documented, scalable, and continuously available application programming interfaces and open machine-readable formats;
b. IT investments must facilitate interoperability, application portability, and scalability across networks of heterogeneous hardware, software, and communications platforms;
c. Information systems, technologies, and processes shall facilitate accessibility under the Rehabilitation Act of 1973, as amended; in particular, see specific electronic and IT accessibility requirements commonly known as “section 508” requirements (29 U.S.C. § 794d);
d. Records management functions and retention and disposition requirements must be fully incorporated into information life cycle processes and stages, including the design, development, implementation, and decommissioning of information systems, particularly Internet resources to include storage solutions and cloud-based services such as software as a service, platform as a service, and infrastructure as a service; and
e. IT investments use an Earned Value Management System (EVMS) and Integrated Baseline Review, when appropriate, as required by FAR Subpart 34.2. Per Circular No. A-11 “All major acquisitions with development effort will include the requirement for the contractor to use an EVMS that meets the guidelines in ANSI/EIA Standard—748 to monitor contract performance.” (OMB Circular No. A–11 (2016) - Page 18 of Capital Programming Guide)]. When an EVMS is required, agencies must have a documented process for accepting a contractor’s EVMS. Agencies are encouraged to share information about their acceptance process with other agencies and to consider recognizing each other’s acceptance of an EVMS so that a contractor is not required to complete a duplicative process. When an EVMS is not required, implement a baseline validation process as part of an overall investment risk management strategy consistent with OMB guidance.

1.7 CPIC Integration with Other Management Processes

The CCA and the FITARA governs the CPIC process and emphasizes three areas of focus: effective CPIC; adherence to an IT plan and EA; and the resource planning to accomplish both of these objectives. To understand the role of IT capital planning within the IT management process, it is important to recognize how it complements other BLM planning and management processes. What follows is a summary of linkages between the BLM IT CPIC process and related management processes and events.

Roadmapping and Configuration Management (CM)

The Department of the Interior uses an IT Roadmapping process rather than a full Enterprise Architecutre (EA) process. Roadmapping implementation in combination with effective CM controls provides vital structure to the overall CPIC process. When used with other portfolio management techniques, these disciplines help ensure that senior management decision making processes are well designed and documented. Roadmapping provides a framework which facilitates analysis for effectively depicting consolidation opportunities from seemingly dissimilar projects. Information which can readily be derived from an effective CM program can identify re-useable products, illustrate potential integration and interoperability risks, shorten development and testing cycles, and offer greatly improved chances for a project’s eventual success. For ongoing investments, both the Roadmapping and CM assess if existing investments are still meeting business needs and identify replacement candidates, if required. CM also provides additional O&M monitoring capabilities providing useful inputs into future CPIC analysis.

IT Security

IT security is an inherent component of the CPIC process. All IT investments must demonstrate that costs for appropriate IT security controls and privacy are incorporated into the lifecycle planning of all systems in a manner consistent with the FISMA and the OMB guidance for IT investments. Cost effective security of the BLM information systems must be an integral component of business operations.

Per NIST SP 800-53 'Security and Privacy Controls for Federal Information Systems and Organizations', asset management 'security controls' such as Configuration Management-8 (CM-8) Information System Component Inventory' are an 'integral part' of information system updates. As indicated in NIST SP 800-65 'Integrating IT Security into the Capital Planning and Investment Control Process', FISMA 'effectively integrates IT security and capital planning because agencies must document resource and funding plans for IT security'.

IT security is a critical element of the business case criteria for the review and evaluation of investments through the IT CPIC process.

Each business case should include costs associated with all aspects of the Security and the Privacy program normally occurring expenses. For example: ongoing cyclical assessment and authorization (previously known as certification and accreditation), risk identification and mitigation activities, privacy impact assessment, and day-to-day investment level security operations activities.

Budget Formulation and Execution

In accordance with the requirements of OMB Circular A-11, Section 53[7] the BLM is required to annually submit its IT investments as part of the DOI's budget request. This will include existing investments, enhancements to existing investments, and new initiatives. During the budget process, the rationality of the cost estimates is examined and Agencies are held accountable for meeting the cost goals of their IT investment portfolio.

An Alternative Analysis (AA) is conducted for each IT investment and the selection and prioritization of alternatives is based on a Cost Benefit Analysis (CBA). The CBA uses a systematic analysis of expected benefits and costs. Estimates of risk-adjusted costs and benefits show definitively the performance, budget changes, and risk inherent in undertaking the investment.

The BLM's IT CPIC process is closely aligned to its budget cycle (Section 7.3.1). This includes reviews by the respective sponsors of the IT-related funding requests developed by the BLM during the formal budget formulation process. All budget requests will be reviewed and prioritized based on projected requirements as approved by the ITIB. New investments are justified based on the need to fill a gap in the BLM's ability to meet strategic goals and objectives while providing risk-adjusted cost and schedule goals with measurable performance benefits.

Modular Approaches

Modular approaches involve dividing investments into smaller parts in order to reduce investment risk, deliver capabilities more rapidly, and permit easier adoption of newer and emerging technologies. Modular development focuses on an investment, project, or activity of the overall vision and progressively expands upon the BLM's capabilities, until the overall vision is realized. Investments may be broken down into discrete projects, increments, or useful segments, each of which are undertaken to develop and implement the products and capabilities that the larger investment must deliver. [8]

By following a modular approach, the BLM can recognize the following benefits:

- Delivery of usable capabilities that provide value to customers more rapidly as agency missions and priorities mature and evolve;
- Increased flexibility to adopt emerging technologies incrementally, reducing the risk of technological obsolescence;
- Decreased overall investment risk as agencies plan for smaller projects and increments versus "grand design" (each project has a greater overall likelihood of achieving cost, schedule, and performance goals than a larger, all-inclusive development effort);
- Creation of new opportunities for small businesses to compete for the work;
- Greater visibility into contractor performance. Tying award of contracts for subsequent Task Orders to the acceptable delivery of prior projects provides agencies better visibility into contractor performance and allows a greater opportunity to implement corrective actions without sacrificing an entire investment;
- An investment can be terminated with fewer sunk costs, capping the risk exposure to the agency when the following occurs:
    - priorities change,
    - a technology decision does not work, or
    - a contractor's performance does not deliver results.

[7] Appendix C-12
[8] Appendix C-7

Agile Software Development

Agile software development is a method of software development that utilizes an iterative development process, designs services based on real user needs, and constantly improves software from user feedback. Agile software development principles apply to both pre-award and post-award contexts. The method is based on iterative and incremental processes and collaboration among a team. It is a methodology for the creative process that anticipates the need for flexibility and applies a level of pragmatism into the delivery of the finished product. The focus is on keeping code simple, testing often, and delivering functional bits of the application as soon as they are ready.[9]

Per the OMB Digital Services Playbook, the Agile software development is the preferred methodology for software development contracts that contribute to the creation and maintenance of digital services, whether they are websites, mobile applications, or other digital channels. It supports frequent changes, updates, and enhancements to the software. By breaking up the development process into small, manageable pieces – each with desired segments of functionality, and having end users involved throughout the process – and guided by the Product Vision, users receive software that better meets their needs (in terms of both functionality and usability) without wasting money and time on unused or unusable features.

Earned Value Management (EVM)

EVM is a program management technique that uses an investment's past performance and work to evaluate and forecast the investment's future performance. This enables the PM to make changes that keep the investment at or bring the investment closer to planned expectations.

Earned value analysis is part of a performance based management system required by OMB for all IT investments. Earned Value analysis is built into the business case (BC) template. The PM plans Work Breakdown Structure (WBS) tasks and builds budget estimates for each task in the project plan. As the plan is executed, the PM tracks actual progress and expenditures at the completion of each WBS against planned figures to obtain cost and schedule variances (SV). These variances can then be used to identify schedule and cost-over or under-runs so they can be resolved as quickly as possible. Additional information about the EVM is available at the BLM CPIC website[10].

1.8 Thresholds

All BLM IT systems development, maintenance efforts, and infrastructure computing resources must comply with this CPIC Handbook.

All IT investments that meet the following thresholds must be reviewed and approved by the ITIB:

- Any investment that is a Major Investment or General Support System;
- Any investments with a total lifecycle value of greater than $500,000
- Any investment that affects multiple States/Centers, or multiple business areas.

Major Investment

[9] Appendix C-8

[10] Appendix-D

Per the OMB, a Major IT investment refers to an IT investment requiring special management attention because of its importance to the mission or function to the government; significant program or policy implications; high executive visibility; high development, operating, or maintenance costs; unusual funding mechanism; or defined as major by the agency's capital planning and IT investment control process. The OMB may work with the agency to declare IT investments as Major IT investments. Agencies should consult with their assigned OMB analysts regarding which IT investments are considered "Major." IT investments not considered "Major" are considered "Non-Major." The DOI's Major IT investments include at least one of the following:

- IT investments previously reported to the OMB as Major IT investments unless approved by the DOI for Non-Major categorization or decommissioning;
- $5M annual cost or greater than $35M lifecycle cost;
- Importance to the mission or significant role in administration of programs, finances, property, or other resources;
- Integral part of the DOI's Enterprise Roadmap;
- Mandated by legislation or executive order, or identified by the Secretary as critical;
- Greater than $1M Development, Modernization and Enhancement (DME) in the current fiscal year (FY);
- High risk as determined by the OMB, Government Accountability Office (GAO), Congress and/or the CIO; and
- E-Government, Departmental, cross-cutting/Enterprise-wide (across more than one office or bureau).

1.9 Process Overview

The CPIC is a structured process in which proposed and ongoing IT investments are continually monitored and evaluated throughout their lifecycle. Successful investments as well as terminated or delayed investments are evaluated to assess the impact on future proposals and to compile lessons learned. The BLM's CPIC contains four phases for a systems' lifecycle. These are pre-select, select, control, and evaluate. As detailed in this document, each phase contains the following common elements:

- Purpose – a description of the objectives of the project expected to be completed in each phase;
- Entry Criteria - describes the requirements and thresholds for entering the given phase;
- Process - the type of justification, planning, and review that will occur in the phase;
- Exit Criteria – documentation of the action, evaluation methodology, and associated metrics used to determine the project is successful and may reasonably proceed to the next phase.

Completing one phase is necessary before beginning another. The work to document the project activities and provide justifications for the ITIB review is undertaken by the project staff. Each phase is overseen by the ITIB, which ultimately approves or rejects an investment's advancement to the next phase. This ensures that each investment receives the appropriate level of managerial review, coordination, and accountability.

At the highest level, the CPIC process can be represented as a circular flow of BLM's IT investments through four sequential phases as shown in Figure 1-2 and described below:

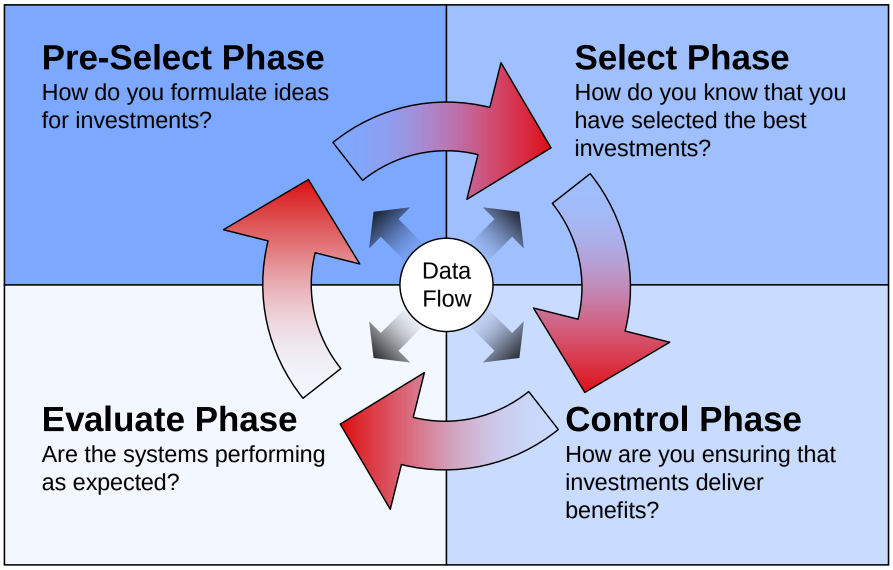

Pre-Select Phase
How do you formulate ideas for investments?
Select Phase
How do you know that you have selected the best investments?
Data Flow
Evaluate Phase
Are the systems performing as expected?
Control Phase
How are you ensuring that investments deliver benefits?

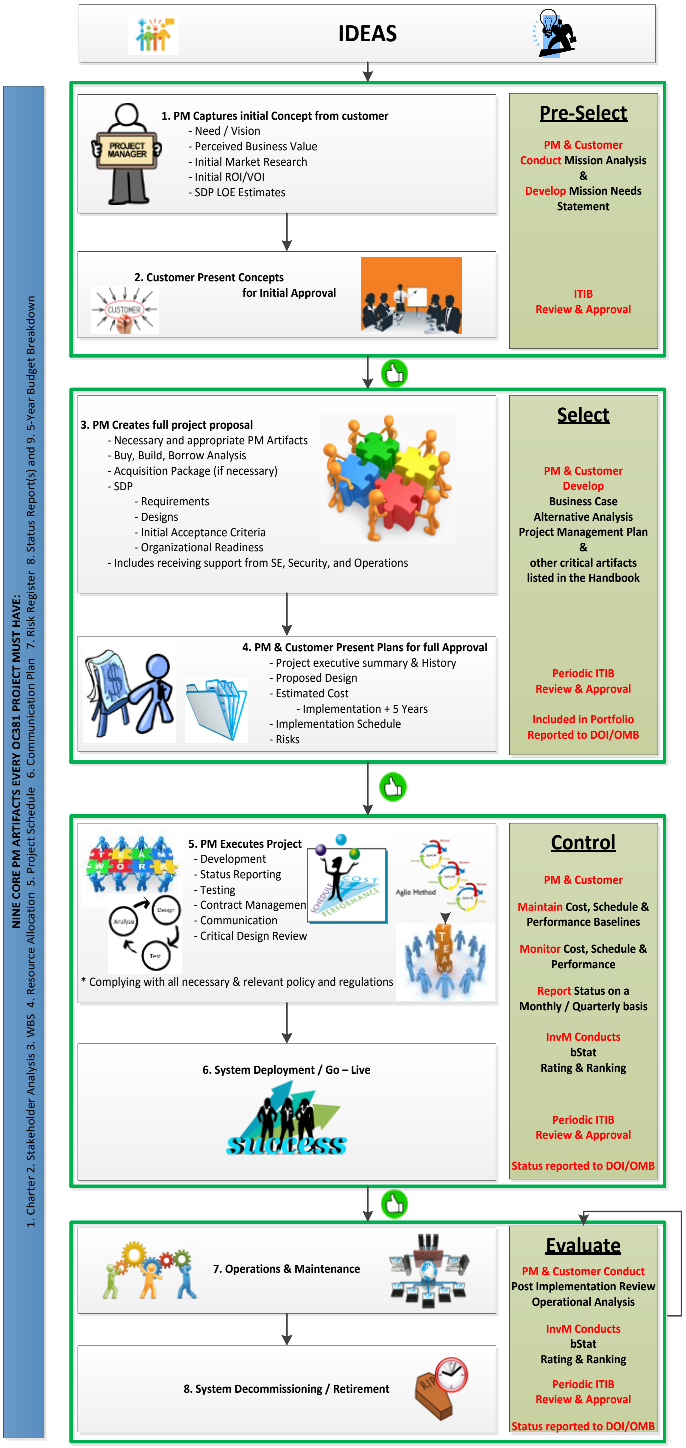
Figure 1-2: CPIC Information and Process Flow

- **Pre-Select Phase:** In the initial screening process, when IT investments are proposed, executive decision-makers assess each proposed investment's support of the BLM's strategic and mission needs and potential for business improvement. If sufficient benefit potential has been demonstrated, further analysis is carried out to prepare the investment for more detailed review in the Select Phase;
- **Select Phase:** In this phase, IT investment comparison, evaluation, and prioritization are performed. An analysis is conducted with the ITIB selecting and prioritizing IT investments that best support the BLM's mission. Prior to selection, details of how the application can be integrated into the current BLM technical operating environment and architecture will also be addressed. Once approved, the project will officially transition to the OMB's prescribed portfolio management process;
- **Control Phase:** Through timely oversight, quality control, and executive review, the BLM ensures that IT initiatives are executed and developed according to pre-approved schedules and milestones in a disciplined, well-managed, and consistent manner.

Evaluate Phase: In this phase, investments are assessed to determine if planned objectives are being met. Actual results of the implemented projects are compared to forecasted expectations to evaluate investment performance. This is done to assess the investment's impact on mission performance, identify any investment changes or modifications that may be needed, and revise the investment management process based on lessons learned. Matured systems are evaluated to ascertain their continued effectiveness in supporting mission requirements, cost effectiveness of continued maintenance support, potential technological opportunities or upgrade, and if they should be considered for retirement or replacement.

Investment Management and NOC's Project Management Processes

Figure 1-3 depicts the mapping between the Investment Management processes and the NOC's Project Management processes. Chapters 2-5 of this handbook describes in details the roles, responsibilities and deliverables of each of the CPIC phases and the corresponding responsibilities of the NOC's PM.



IDEAS

NINE CORE PM ARTIFACTS EVERY OC381 PROJECT MUST HAVE:
1. Charter 2. Stakeholder Analysis 3. WBS 4. Resource Allocation 5. Project Schedule 6. Communication Plan 7. Risk Register 8. Status Report(s) and 9. 5-Year Budget Breakdown

1. PM Captures initial Concept from customer
- Need / Vision
- Perceived Business Value
- Initial Market Research
- Initial ROI/VOI
- SDP LOE Estimates

2. Customer Present Concepts for Initial Approval

Pre-Select

PM & Customer Conduct Mission Analysis & Develop Mission Needs Statement

ITIB Review & Approval

3. PM Creates full project proposal
- Necessary and appropriate PM Artifacts
- Buy, Build, Borrow Analysis
- Acquisition Package (if necessary)
- SDP
  - Requirements
  - Designs
  - Initial Acceptance Criteria
  - Organizational Readiness
- Includes receiving support from SE, Security, and Operations

4. PM & Customer Present Plans for full Approval
- Project executive summary & History
- Proposed Design
- Estimated Cost
  - Implementation + 5 Years
- Implementation Schedule
- Risks

Select

PM & Customer Develop Business Case Alternative Analysis Project Management Plan & other critical artifacts listed in the Handbook

Periodic ITIB Review & Approval

Included in Portfolio Reported to DOI/OMB

5. PM Executes Project
- Development
- Status Reporting
- Testing
- Contract Managemen
- Communication
- Critical Design Review

* Complying with all necessary & relevant policy and regulations

6. System Deployment / Go – Live

Control

PM & Customer

Maintain Cost, Schedule & Performance Baselines

Monitor Cost, Schedule & Performance

Report Status on a Monthly / Quarterly basis

InvM Conducts bStat Rating & Ranking

Periodic ITIB Review & Approval

Status reported to DOI/OMB

7. Operations & Maintenance

8. System Decommissioning / Retirement

Evaluate

PM & Customer Conduct Post Implementation Review Operational Analysis

InvM Conducts bStat Rating & Ranking

Periodic ITIB Review & Approval

Status reported to DOI/OMB

WAIVER PROCESSES:
Provides a standardized guideline for requesting an exception to the process, procedure and / or regulation. Available to fast-track, out-of-cycle or emergency projects.

Figure 1-3: Investment Management and NOC's Project Management Processes

2 *Pre-Select Phase*

2.1 Purpose

The Pre-Select Phase provides a process to assess a proposed investment and determine the degree to which it supports the BLM's operating plan and mission. During this phase the business or mission need is identified and the relationships to the BLM's strategic planning efforts are established. The Pre-Select Phase enables the project proponent to begin defining business needs and associated capabilities, risks, benefits, and costs.

2.2 Entry Criteria

Prior to entering the Pre-Select Phase, the Business Managers generate ideas for the next budget cycle based on BLM missions and strategic goals. Proposed investments must have a new concept which addresses the BLM mission needs. It is expected to include an IT component.

2.3 Process

During the Pre-Select Phase, a Mission Needs Statement (MNS) is prepared (template is available on BLM CPIC website[11]). Completion of the MNS results in the identification of a business opportunity and consideration of an IT solution. The level of required detail varies and should be commensurate with the magnitude, complexity, and cost of the proposed investment. The analysis and corresponding development of a MNS is closely linked to the BLM's strategic planning process.

Figure 2-1 provides a summary of the Pre-Select Phase process, as well as the individual(s) and/or group(s) responsible for completing each process step.

[11] Appendix-D

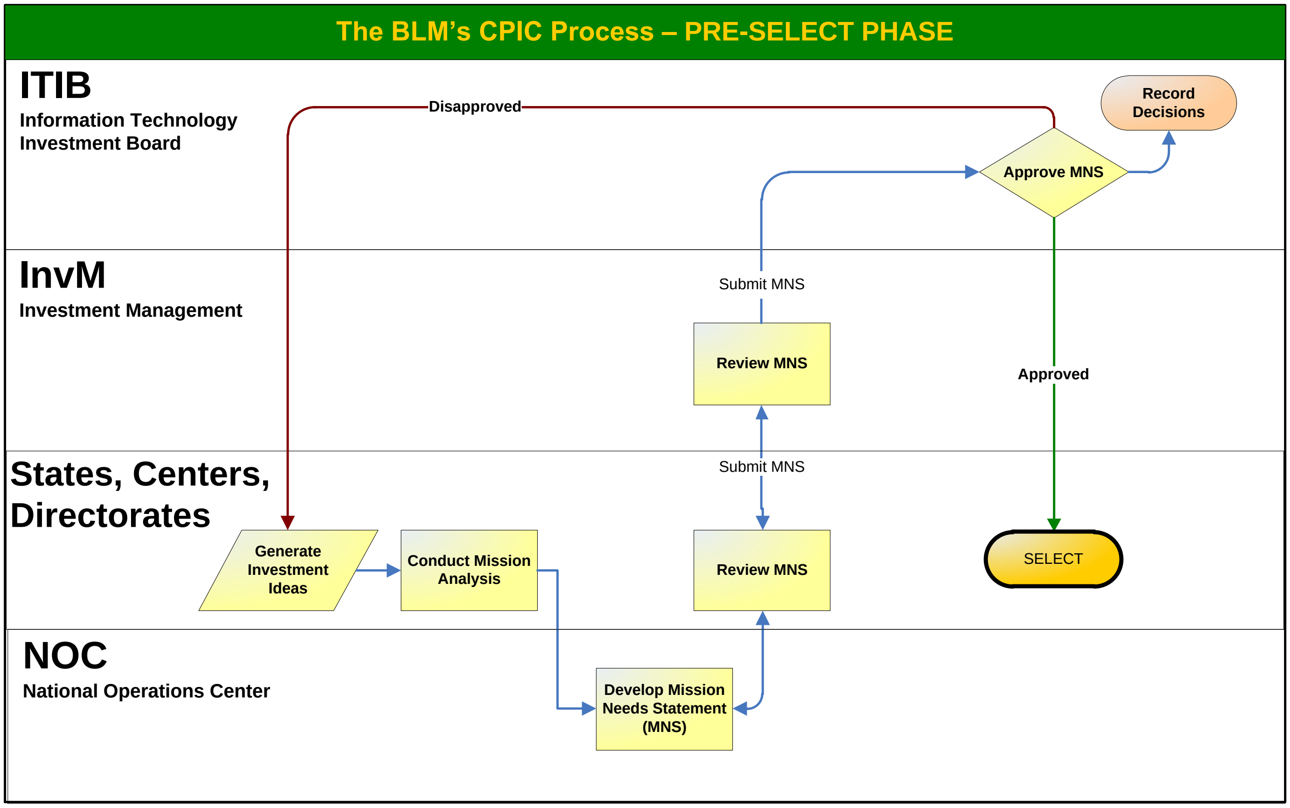

The BLM's CPIC Process – PRE-SELECT PHASE
ITIB
Information Technology Investment Board
InvM
Investment Management
States, Centers, Directorates
NOC
National Operations Center
Disapproved
Record Decisions
Approve MNS
Submit MNS
Review MNS
Approved
Submit MNS
Generate Investment Ideas
Conduct Mission Analysis
Review MNS
SELECT
Develop Mission Needs Statement (MNS)

Figure 2-1: Pre-Select Phase Process

2.3.1 Generate Investment Ideas

New ideas or recommendations for enhancement to a current investment are submitted by the Business Managers, Investment Sponsors, or PMs to their ADs, SDs, or CDs (center) for approval.

2.3.2 Conduct Mission Analysis

A mission analysis is a strong, forward-looking analytical activity to evaluate the capacity of the BLM's assets to satisfy existing and emerging demands for services.

The mission analysis enables the BLM to assess and prioritize the most critical capability shortfalls and best technology opportunities to improve overall security, capacity, efficiency, and effectiveness in providing services to customers. Mission analysis is conducted within the framework of the BLM's long-range strategic goals. Concurrently, the mission analysis contributes strongly to the evolution of strategic planning and the BLM's IT architecture development.

The mission analysis allows the BLM to identify critical needs. Also identified are preliminary resource allocation to specific mission needs within the context of the BLM's overall resource projections and within the constraints of future BLM's budget authority projections. The results of the mission analysis provide micro- and macro-level views as well as key data for strategic planning efforts. More refined resource quantification, including the acquisition of hardware, software, and service contracts, is conducted during the Business Case development in the Select Phase if the investment is selected as part of the BLM's portfolio. The resource estimate (hardware, software, service contracts and staff) is a function of the benefit to the BLM and the mission area, the cost of not addressing the need (e.g., poor customer responsiveness, increased maintenance cost, lost productivity, etc.), and the likely extent of required additional investment or changes to the BLM's infrastructure.

If the mission analysis reveals a non-IT solution (e.g., a policy change, operational procedural change, or transfer of systems between sites) that can satisfy a capability shortfall and can be achieved within approved budgets, it can be implemented as a non-IT initiative, and will not be managed within the CPIC process.

A complete mission analysis should also identify the business drivers (e.g., the BLM's mission, vision, goals, objectives, and tactical plans). Business drivers often involve the need to assist customers in a particular service area such as recreation on public lands.

Once the key business drivers have been identified, a business requirements analysis is conducted. The business requirements analysis identifies how personnel conduct business activities to fulfill mission requirements, meet objectives, and perform tactical plans.

While MNSs will be generated from the mission analysis, any individual or organization may propose an investment based on a perceived capability shortfall or technological opportunity. Examples of potentially valid needs that could originate outside BLM lines of business include those related to socioeconomic and demographic trends, the environment, statutory requirements, or an industry-developed technological opportunity. These shortfalls and opportunities should be communicated to the project sponsor. The project sponsor will then determine how the mission analysis should be conducted to validate, quantify, and prioritize the proposed need.

The following four principal activities must be addressed while conducting the mission analysis:

1. Identify and quantify projected demand for services. This should be based on input from strategic planning for services needed in the future as well as performance and supportability trends of current systems and projected technological opportunities that will enable the BLM to perform its mission more efficiently and effectively.
2. Identify and quantify existing and projected services based on information from field organizations, the EA, and IT asset inventory that defines what is in place and what is approved for implementation. Special consideration should be given to IT Modernization Blueprints, Cloud Services and Commercial off the Shelf Software (COTS) to determine whether investments identified may meet or might efficiently be extended to meet the newly identified requirement.
3. Identify, analyze, and quantify capability shortfalls (e.g., the difference between demand and supply) and technological opportunities to increase quality of service, efficiency, and effectiveness.
4. Identify the user and customer base affected.

When the analysis identifies a capability shortfall or technological opportunity, the results are summarized in the MNS (template is available on the BLM CPIC website[12]). The MNS must clearly describe the capability shortfall and the impact of not satisfying the shortfall or the technological

[12] Appendix D

opportunity and the increase in efficiency it will achieve. The MNS also must assess the criticality and timeframe of the need and estimate the resources the BLM should commit to resolving the shortfall based on merit, criticality, and the scope of likely changes to the BLM's IT asset base. This information forms the basis to establish the priority of this need within the context of an enterprise view of all the BLM's needs.

The MNS is a summary document that describes a new opportunity or operational problem and presents the major decision factors that the ITIB should evaluate when considering the need satisfied by the proposed investment.

2.3.3 Review MNS

The InvM, with input from Subject Matter Experts (SME), verifies the current and planned capabilities that are proposed in the MNS and ensures that no redundant IT investments provide similar capabilities. Business process owners must simplify or otherwise redesign their existing processes before initiating new systems investing in new IT programs. Plans for redesign or business process re-engineering (BPR) should be discussed as part of the MNS. The InvM reviews the MNS before final submission to the ITIB. If any modifications or updates are required, the MNS is referred back to the project sponsor for review and update. Final review results are presented to the ITIB for decision.

2.3.4 MNS Approval

The ITIB will review and evaluate the submitted MNS. Approved investments are progressed to the Select Phase for business case development. The ITIB's decision is recorded in the minutes and appropriate parties are notified. A disapproved MNS is sent back to the project sponsor.

2.4 Exit Criteria

Prior to exiting the Pre-Select Phase, the sponsor must obtain ITIB approval of the MNS.
Table 2-1 provides a summary of the documents generated during the Pre-Select Phase process and if the document requires approval or is required only for filing and record keeping purposes.

Document	Required For File	Required For ITIB Approval
MNS	X	X
ITIB Decision & Meeting Minutes	X	

Table 2-1: Summary of documents generated during the Pre-Select Phase

3 Select Phase

3.1 Purpose

In the Select Phase, the BLM ensures the IT investments that best support the mission are chosen. Trained, experienced, qualified, and certified PMs are selected and risk management is initiated. PMs assigned to Major Investments must be senior-level certified FAC-P/PM. Other PMs must be, at a minimum, mid-level certified FAC-P/PM. Investments are reviewed to ensure no duplication of e-Government initiatives or existing system applications. Individual investments are evaluated in terms of technical alignment with other IT systems and projected performance as measured by Cost, Schedule, Benefit, and Risk (CSBR). For each investment, a high level WBS with proposed milestones and review schedules is established.

In this phase, the BLM prioritizes each investment (section 7.4) and decides which investments will be included in the portfolio. Business case submissions are assessed against a uniform set of evaluation criteria and thresholds as identified in OMB Circular A-11, Part 7—Planning, Budgeting, Acquisition, and Management of Capital Assets. The investment's CSBR are then systematically scored using objective criteria and ranked and compared to other investments. Finally, the BLM's ITIB decides on investments that will be included in the BLM's portfolio.

3.2 Entry Criteria

Prior to entering the Select Phase, investments must have an ITIB approved MNS.

3.3 Process

The Select Phase begins with an ITIB approved MNS and moves through the development of the Business Case, Acquisition Plan (AP), Risk Management Plan (RMP), performance measures, and a Project Management Plan (PMP). These supporting documents lay a foundation for success in the subsequent phases. The Select Phase culminates in a decision whether or not to proceed with the investment.

Figure 3-1 provides a summary of the Select Phase process as well as the individual(s) and/or group(s) responsible for completing each process step.

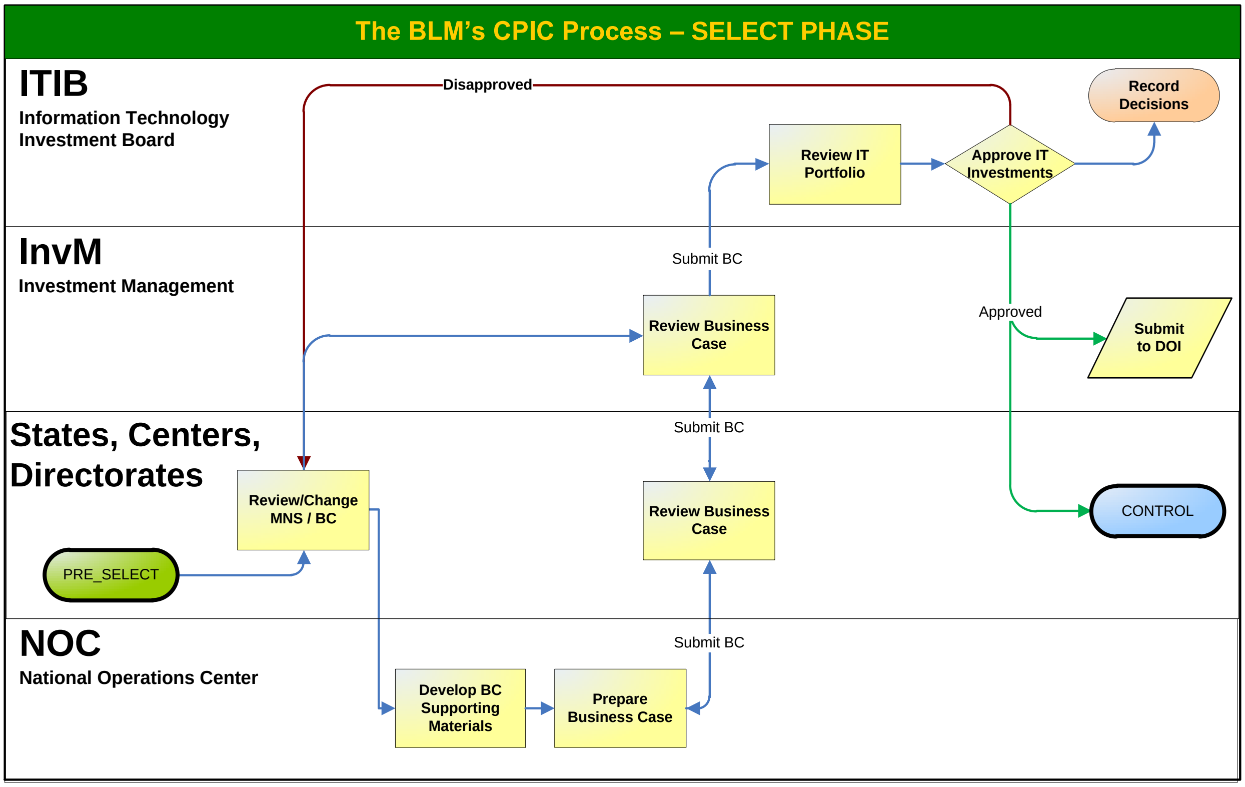


Figure 3-1: Select Phase Process Steps

3.3.1 Review the MNS

The Investment Sponsor and Business Manager reviews the MNS and other documentation completed during the Pre-Select Phase and are responsible for making any necessary changes.

3.3.2 Develop Business Case and Supporting Materials

The PM prepares the Business Case and supporting materials for the Business Case. The Investment Sponsor ensures that, for each investment, the below listed documents, and activities are completed and the results are submitted to the InvM (Guidance and document templates are available on the BLM CPIC website[13]). The InvM may assist with coordinating responses to various sections of the Business Case with the SME as needed. The below listed documents are living documents and will be continuously updated as the investment moves through the CPIC lifecycle. Not all documents will be required for all Business Cases. The InvM will work with the PM to identify the required documents.

__Project Management and Planning Profile:__

[13] Appendix-D

- Project Charter
- Project Management Plan (initial draft)
- AP and strategy (initial draft)
- High level WBS with proposed milestones and review schedules

Business Profile:

- Business Case with Performance Measures and MNS
- Business Process Reengineering (BPR) Studies
- Concept of Operations Plan
- Stakeholder Identification and Requirements
- Functional Requirements (initial draft)
- Feasibility Study

Risk Profile:

- RMP (initial draft)

Financial Profile:

- Return on Investment (ROI) and CBA
- Update lifecycle cost projections
- Alternatives Analysis
- Funding Source Identification

Technological Profile:

- Technical Requirements
- Security Plan
- Relationship to existing systems (dependencies)
- Prototype or pilot plans

3.3.3 Review Business Case

The Business Manager and Sponsor reviews and approves the Business Case and Supporting Materials and submits them to the InvM. The InvM reviews the Investment for compliance with BLM strategic, legislative, and budgetary goals. The InvM uses standard criteria to objectively compare investments based on the data presented and scores the projects using the criteria (section 7.4). Review results are presented to the ITIB for decision.

3.3.4 Review of the BLM IT Portfolio by the ITIB

The ITIB reviews the IT investment portfolio, recommendations and suggestions from the business case review, and other assessments. The ITIB uses a standard set of criteria (section 7.4) to prioritize and analyze the investments and to optimize the IT Portfolio based on value, business analysis, risks, and alignment.

3.3.5 Approve IT Investments

After reviewing the portfolio, the ITIB makes final investment decisions. If the investment is approved, it will progress to the Control Phase where funding can be requested or existing funding reprogrammed for development and implementation. The ITIB's decision is recorded and appropriate parties are notified. If the business case is disapproved, it is returned to the sponsor for corrective actions.

3.3.6 Submit to the DOI

The InvM submits approved business cases of Major investments to the DOI. For the DOI to consider an IT initiative for inclusion in the overall DOI IT portfolio, it must be reviewed, approved, and vetted through the CPIC process. In the interim, the InvM performs the following functions:

- Self Scoring the business cases (section 7.4);
- Preparing budget and supporting materials;
- Revising baseline cases based on new guidelines or changes from the OMB.

3.4 Exit Criteria

Prior to exiting the Select Phase, investments must have executed the following activities:

- Established performance goals and quantifiable performance measures;
- Developed a high level project plan which details quantifiable plans and objectives such as high level acquisition schedule, project deliverables, and costs;
- Identified CSBR;
- Established security, Section 508 (IT accessibility), complete Privacy Impact Assessments (PIA);
- Documented data requirements including transition and implementation strategies;
- Established an ITIB investment review schedule for the Control Phase;
- Finalized the project charter with approval from the project sponsor and the ITIB;
- Obtained ITIB approval to enter the Control Phase.

Table 3-1 provides a summary of the documents generated during the Select Phase process and if the document requires approval or is required only for filing and record keeping purposes.

Document	Required For File	Required For Approval
Business Case*	X	X
Supporting Documents*	X	X
* Living documents that will get updated as the investment proceeds through the CPIC lifecycle		

Table 3-1: Summary of documents generated during the Select Phase

4 Control Phase

4.1 Purpose

The objective of the Control Phase is to ensure, through timely oversight, quality control, and executive review, that IT initiatives are implemented in a disciplined, well-managed, and consistent manner. Investments should be closely tracked against the various components identified in the initial Project Management Plan. This phase also promotes the delivery of quality products and results in initiatives that are completed within scope, on time, and within budget. During this process, the ITIB monitors the progress and performance of ongoing IT investments against projected cost, schedule, performance, and delivered benefits. For major investments, the BLM also submits a quarterly report to the DOI for additional oversight.

Based on quarterly control reviews, the ITIB will conduct a portfolio analysis to determine the performance of the BLM's IT portfolio. The reviews focus on ensuring that projected benefits are being realized; cost, schedule, and performance goals are being met; risks are minimized and managed; and the investment continues to meet strategic needs. Depending on the review's outcome, decisions may be made to continue, modify, or terminate investments, suspend funding, or make future funding releases conditional on corrective actions.

4.2 Entry Criteria

Prior to entering the Control Phase, investments must satisfy the Select Phase exit criteria:

- Established performance goals with quantifiable measures;
- Formulated a high level project plan which details quantifiable objectives such as a high level acquisition schedule, project deliverables, and costs;
- Identified initial costs, schedule, benefits, and risks;
- An approved funding plan;
- Established security, Section 508 (IT accessibility), Privacy Act assessment, data, and architecture goals and measures;
- Obtained ITIB approval to enter the Control Phase.

4.3 Process

Throughout the Control Phase, the PMs submit Status Reports (template is available on the BLM CPIC website[14]) to the InvM. In turn, the InvM provides the ITIB with investment reviews to assist them in monitoring all investments in the portfolio. The Status Reports provide an opportunity for PMs to raise issues concerning the IT developmental process, including security, telecommunications, enterprise architecture alignment, e-Government, GPEA compliance, and Section 508.
The PM uses an earned value management system (EVMS) to evaluate project performance and report variance.

All Major investments are required to provide cost and schedule baseline and performance information to the InvM on a monthly basis. All Non-Major investments are required to provide cost and schedule baseline and performance information to the InvM on a quarterly basis. Ongoing performance reporting enables InvM to conduct investment and portfolio-level analysis in accordance with the OMB reporting requirements.

A Corrective Action Report (CAR) (template is available on the BLM CPIC website[15]) is required if the project performance variance exceeds ten (10) percent from the project's established baseline or the ITIB is otherwise dissatisfied with project progress.

[14] Appendix-D
[15] Appendix-D

Figure 4-1 provides a summary of the Control Phase process as well as the individual(s) and/or group(s) responsible for completing each process step.

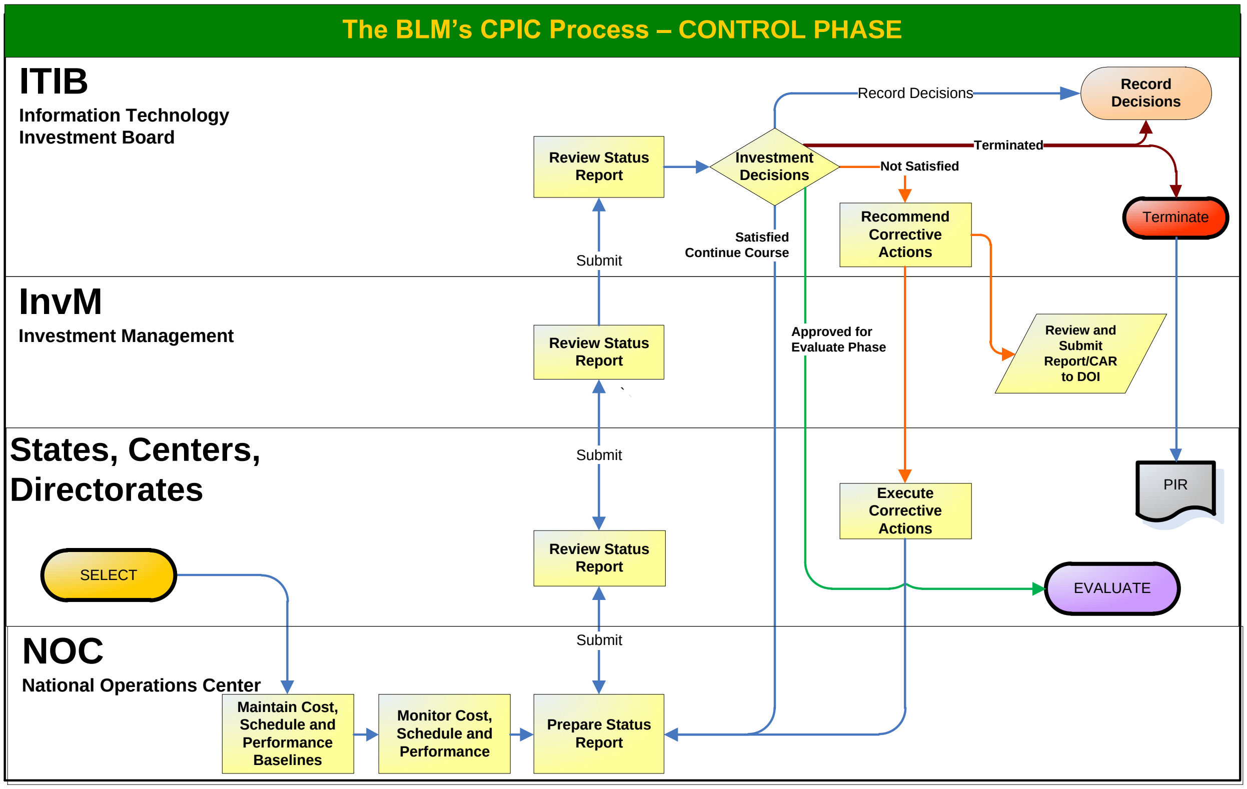

The BLM's CPIC Process – CONTROL PHASE
ITIB
Information Technology Investment Board
InvM
Investment Management
States, Centers, Directorates
NOC
National Operations Center
SELECT
Maintain Cost, Schedule and Performance Baselines
Monitor Cost, Schedule and Performance
Prepare Status Report
Submit
Review Status Report
Submit
Review Status Report
Submit
Review Status Report
Investment Decisions
Record Decisions
Record Decisions
Terminated
Not Satisfied
Satisfied Continue Course
Recommend Corrective Actions
Terminate
Approved for Evaluate Phase
Review and Submit Report/CAR to DOI
Execute Corrective Actions
PIR
EVALUATE

Figure 4-1: Control Phase Process Steps

4.3.1 Maintain Project Costs, Schedule, and Technical Baselines

The DOI Directive 2012-006, "Information Technology Investment Performance Measurement Baseline Management Policy," requires all Major IT investments to have a baseline reflecting the known lifecycle. An approved IT investment baseline constitutes an agreement between the BLM and DOI on the future plan for IT investment activities based on the current environment. An approved baseline does not constitute the DOI approval of IT investment funding beyond the budget year (BY). The PM oversees all aspects of the IT investment and is responsible for the implementation of associated plans that were developed in the Select Phase. The PM also follows the established procedures and practices to monitor performance and ensures that the Integrated Project Team (IPT) is apprised of any new or existing internal risks based upon review of the WBS, project plan, risk checklist, and stakeholder interviews. The PM monitors financial, technical, operational, schedule, legal and contractual, and organizational risks while ensuring all budget documents remain current. The PM provides quarterly updates to the sponsor and/or ITIB on the investment's status and cost, schedule, and technical baselines while ensuring the project has been realistically planned and project documents remain current.

4.3.2 Monitor Current Project Cost, Schedule, and Technical Information

The PM collects actual information on the resources allocated and expended throughout the Control Phase. The project sponsor ensures that the investment still aligns with the mission and strategic plan. The PM compares the actual information collected to the estimated baselines developed during the Select Phase and identifies root causes for any differences. The PM reviews the security and infrastructure analyses for accuracy. The PM maintains a record of changes to the initiative's technical components including hardware, software, security, and communications equipment.

4.3.3 Investment Artifact Requirements

All IT investments should develop the following artifacts, or update existing artifacts as necessary. The PM and the BM must upload their artifacts to the appropriate folders on the InvM website. The PM and the BM are responsible for providing updated versions (including date of last update) as changes are made or as available throughout the IT investment's lifecycle. The InvM will submit the required artifacts to the DOI and the OMB.

Artifact	Submission Frequency
Investment Charter, including the IPT (if/when projects are added to the investment, Investment charter should be updated).	Submit once, update as needed.
Investment-Level Alternative Analysis and Benefit-Cost Analysis	Submitted at least 2.5 years in advance of contract expiration or at minimum every 3 years once operational.
Risk Management Plan	Every two years.
Operational Analyses (for operational or mixed life cycle systems).	Annually for Major investments and every two years for Non-Major investments.
Post Implementation Review (PIR) Results (investment level or project specific).	As necessary within 6 months after implementation.
Documentation of Investment Rebaseline and Management	As applicable.
Acquisition Plan	Annually.

Table 4-1: IT investments artifacts

4.3.4 Prepare Status Report

On a monthly basis for the Major Investments and quarterly basis for the Non-Major investments, the PM prepares a status report (guidance available at the BLM CPIC website) that provides project status on costs, schedule, and risks. Ongoing performance reporting enables the InvM to conduct investment and portfolio-level analysis in accordance with the OMB's reporting requirements.

Once complete, this status report is submitted to the InvM for review and subsequently provided to the ITIB.

4.3.5 Review Status Report

The InvM evaluates the Status Reports for project performance and prepares findings and recommendations for the ITIB.

4.3.6 ITIB Review of Status Report

Achieving maximum benefits from an investment, while minimizing risks, requires that the investment be consistently monitored and managed for successful results. On a quarterly basis, the ITIB continues to monitor investments making decisions and taking actions to change the course of a particular investment when necessary. The ITIB determines whether to continue, modify, or terminate the project and also if the PM is managing investment cost and SV, mitigating risks, and providing projections for future performance based upon work accomplished to date. The ITIB verifies if the current cost and schedule projections align with the investment.

4.3.7 Investment Decision

The ITIB reviews the Status Reports along with the InvM findings and recommendations and issues one of the four decisions listed below:

1. Continue the investment "as is"
2. Recommend corrective actions – the ITIB may recommend corrective action if:
   - The Project performance variance exceeds ten (10) percent from the project's established baseline;
   - There are constant changes in the requirements and work scope;
   - A particular task on the critical path is missed with no alternative. This may include a major milestone or work product which was missed or delayed;
   - The investment's outcome does not adequately support the mission, business, or security function;
   - Major problems hinder the planned investment development.

   These recommendations are shared with the InvM for incorporation into the monthly submission to the DOI.
3. Rebaseline the investment. PMs, with sponsor concurrence and approval, may request ITIB approval to be re-baselined with new performance targets (scope, schedule, or budget performance goals). The sponsor, by requesting approval from the ITIB for a project re-baselining, is accepting the additional risk and management oversight responsibilities to ensure the investment is delivered within the revised project baseline.
4. Terminate the investment. If the above three options are not applicable or met by the investment, then the ITIB may terminate the investment. If an investment is terminated, the PM prepares and confirms the PIR schedule (section 5.3).

4.3.8 Investment Rebaseline

Rebaselining is required in response to changed requirements, funding changes, or realization that the operative implementation plan is not achievable. This includes the addition, removal, and adjustment of projects and activities to the investments currently approved baseline (cost and/or schedule). A rebaseline constitutes a revised implementation plan with a new milestone schedule.

All rebaselines require AD-BFIRM review and approval, and the respective budget officer must be aware of the change. Rebaselines exceeding a +/-10% change to the performance measurement baseline, or a major change to the technical approach will need the investment teams to provide more detail regarding the rationale and impact of the change, and a meeting between the AD-BFIRM and the investment team may be required for approval.

Investment sponsor must submit all performance measurement baseline change requests through the Performance Baseline Change Request (PBCR) tables exported from Electronic Capital Planning and Investment Control (eCPIC) regardless of the change type and impact. In addition to the proposed PBCR tables, the following associated documents are also required:

1. **Life Cycle Costs and Funding Source tables** exported from eCPIC to Excel to match the funding requested in the baseline change request;
2. **Projects Table exported** from eCPIC to Excel to show any changes to current projects that will result from the PBCR;
3. **Operational Performance Metrics table** exported from eCPIC to Excel to reflect the new operational performance metrics associated with the proposed baseline, as applicable; and
4. **PBCR PowerPoint template** if there is greater than a +/- 10% change to the performance measurement baseline or a major change to the technical approach.

4.4 Exit Criteria

Prior to exiting the Control Phase, investments must complete the following activities:

- Complete investment development, production deployment, and/or implementation;
- Confirm the PIR schedule;
- Obtain ITIB approval to enter the Evaluate Phase.

Table 4-2 provides a summary of the documents generated during the Control Phase process and if the document requires approval or is required only for filing and record keeping purposes.

Document	Required For File	Required For Approval
Project Management Plan	X	X
Status Reports	X	X
PIR Schedule (For investments terminated or approved for Evaluate Phase)	X	
Updated Business Case	X	X

Table 4-2: Summary of documents generated during the Control Phase

5 Evaluate Phase

5.1 Purpose

The purpose of the Evaluate Phase is to compare actual to expected results after an investment is fully implemented. This is done to assess the investment's impact on mission performance, identify any investment changes or modifications that may be needed, and revise the investment management process based on lessons learned. The Evaluation Phase closes the loop of the IT investment management process by comparing actual against estimates in order to assess the performance and identify areas where decision-making can be improved.

The Evaluate Phase focuses on three outcomes:

- Determines whether the IT investment met its performance, cost, and schedule objectives;

- Provides the means to assess mature investments, determine their continued effectiveness in supporting mission requirements, evaluate the cost of continued maintenance support, assess technology opportunities, and consider potential retirement or replacement of the investment.
- Determines the extent to which the CPIC process improved the outcome of the IT investment;

The outcomes are measured by collecting performance data, comparing actual to projected performance and conducting a PIR and OA (Operational Analysis) to determine the system's efficiency and effectiveness in meeting performance and financial objectives.

5.2 Entry Criteria

- The Evaluate Phase begins once a system has been implemented and becomes operational or goes into production. Any investment cancelled prior to being operational must also be evaluated. Prior to entering the Evaluate Phase, investments must have executed the following activities:Complete investment development, and production deployment;
- Confirm the PIR schedule;
- Obtain BLM ITIB approval to enter the Evaluate Phase.

5.3 Process

Investments enter the Evaluate Phase based on the ITIB's decision to either continue the investment, with or without modifications, or to terminate the investment. Investments move to the PIR stage and after a successful PIR to the OA stage. During the PIR, actual performance measures are compared to performance projections made during the Select Phase. Then, "lessons learned" for both the investment and the CPIC process are collected and applied to prior CPIC phases (template and guidance on the BLM CPIC website[16]).

<u>PIR STAGE</u>: From the time of implementation, the system is continually monitored for performance, maintenance activities, costs, resource allocation, defects, problems, and system changes. System stability is also periodically evaluated. The PIR (template is available on the BLM CPIC website[17]) includes a methodical assessment of the investment's costs, performance, benefits, documentation, mission, and level of stakeholder and customer satisfaction.

The PIR process involves reviewing mission needs and project goals, collecting and analyzing cost, schedule, performance and customer satisfaction data, and providing major findings and issues to the InvM. It also provides feedback and incorporates lessons learned.

The PIR is conducted by the project sponsor and PM and results are reported to the InvM and ITIB to provide a better understanding of initiative performance and to assist the project sponsor in directing any necessary initiative adjustments.

[16] Appendix-D
[17] Appendix-D

OA STAGE: During this stage, an OA (template and guidance on the BLM CPIC website[17]) is performed annually for 'Major' investments and every other year for 'Non-Major' investments to determine whether mature systems are continuing to support mission and business requirements.

Figure 5-1 provides a summary of the Evaluate Phase process, both in the PIR and OA stages, as well individual(s) and/or group(s) responsible for completing each process step.

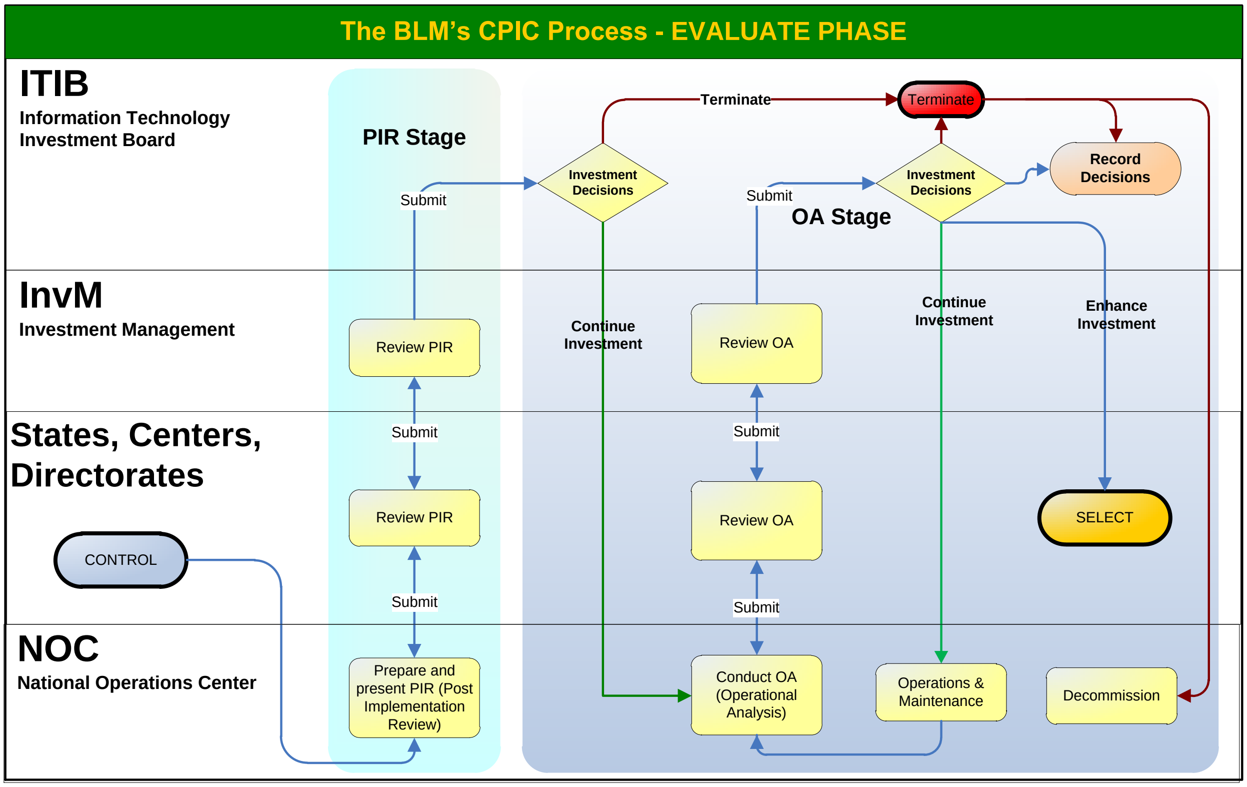


Figure 5-1: Evaluate Phase Process Steps

5.3.1 Prepare and Present PIR

The PIR schedule is determined during the Control Phase. The PIR for a newly deployed initiative should take place six to twelve months after the system is operational. In the case of a terminated system, it should take place immediately because the review will help to define any "lessons learned" that can be factored into future IT investment decisions and activities. In either case, before starting the PIR, the project sponsor develops a PIR plan that details the roles, responsibilities, and schedule for all PIR tasks.

At the heart of the PIR is the IT Investment Evaluation (template and guidance on the BLM CPIC website[18]) in which the project sponsor examines the impact the system has had on customers, business processes, the mission and programs, and the technical capability. As a result of the PIR, the project

[18] Appendix-D

sponsor provides an IT Investment Evaluation Sheet (template and guidance on the BLM CPIC website[18]) to the InvM.

The IT investment evaluation focuses on three areas:

1. Impact to stakeholders: The project sponsor typically measures the impact the system has on stakeholders through user surveys (formal or informal), interviews, and feedback studies. The evaluation data sheet highlights results.
2. Ability to deliver the IT performance measures (quantitative and qualitative). The system's impact to the mission and program should be carefully evaluated to determine whether the system delivered the expected results. This information should be compared to the investment's original performance goals. This evaluation and comparison should also include a review of the investment's security and data performance measures.
3. Ability to meet baseline goals: To determine whether the investment is meeting its baseline goals, the PM should review the following areas:
   - Cost: Present actual lifecycle costs to date;
   - Return: Present actual lifecycle returns to date;
   - Funding Sources: Present actual funds received from planned funding sources;
   - Schedule: Provide original baseline and actual initiative schedule;
   - IT Accessibility Analysis: Determine whether the initiative addresses accessibility for persons with disabilities, how the requirements were managed, and impact on the architecture;
   - Risk Analysis: Identify initiative risks and how they were managed or mitigated, as well as their effects, if any (guidance on the BLM CPIC website);
   - Systems Security Analysis: Identify initiative security risks and how they were managed or mitigated as well as security performance measures;
   - Data Analysis: Determine alignment with the investment's data management plan;
   - Records Management Analysis: Determine compliance with the Records Management policies;
   - Geospatial Analysis: If applicable, determine alignment with the investment's Geospatial requirements.

The project sponsor also prepares and makes a formal PIR presentation to the InvM. The presentation should summarize the investment evaluation and provide a summary of recommendations for presentation to the ITIB.

5.3.2 Review PIR

InvM reviews the PIR results, prepares findings and recommendations, and forwards the package to the ITIB for review

5.3.3 Approve PIR

The ITIB reviews the PIR results of the investment and issues one of the four decisions listed below:

1. Continue the investment "as is" and approve to move to the OA stage;
2. Recommend corrective actions – the ITIB may recommend corrective actions for the following:
   - Project performance variance exceeds ten (10) percent from the project's established baseline;
   - There are constant changes in the requirements and work scope;
   - A particular task on the critical path is missed with no alternative. This may include a major milestone or work product which was missed or delayed;

- The investment's outcome does not adequately support the mission, business, or security function;
- Major problems hinder the planned investment development.

These recommendations are shared with the InvM for incorporation into the monthly submission to the DOI.

3. Rebaseline the investment. PMs, with sponsor concurrence and approval, may request ITIB approval to be re-baselined with new performance targets (scope, schedule, or budget performance goals). The sponsor, by requesting approval from the ITIB for a project re-baselining, is accepting the additional risk and management oversight responsibilities to ensure the investment is delivered within the revised project baseline.
4. Terminate the investment. If the above three options are not applicable or met by the investment, then the ITIB may terminate the investment.

If the investment is approved to remain operational, an OA is prepared. Investments that are not operational are removed from the BLM's portfolio. The ITIB's decision is recorded and appropriate parties are notified.

5.3.4 Conduct OA

The project sponsor and the PM conduct an OA (template is available on the BLM CPIC website[19]) to assess the cost and extent of continued maintenance and upgrades. The OA should include a trend analysis of O&M costs and a quantification of maintenance releases. Costs for Government employees as well as any customer cost should be included in all cost estimates and analysis. OA is conducted annually for 'Major' and every other year for 'Non-Major' investments.

The project sponsor and PM also conduct an analysis to determine if the system is continuing to meet mission requirements and supports the BLM's evolving strategic direction. The mission analysis process identified in the Pre-Select Phase and the MNS provide a framework to assist in the mission analysis for the OA Stage. This includes an analysis of the performance measurements accomplished.

The PM assesses the technology and determines potential opportunities to improve performance, reduce costs, meet Security, Data, Privacy, Records, and GIS requirements, and to ensure alignment with BLM's strategic direction.

Alternatively, the ITIB may decide to enhance an investment and return it to the Select Phase. The ITIB also reviews InvM recommendations to rate and rank the investment as a part of the ITIB's function of annual reselection of BLM's IT portfolio (section 7.3). Systems that are not annually reselected will be terminated and removed from the portfolio. InvM then informs the project sponsors of the ITIB decisions and recommendations.

5.3.5 Review OA

InvM reviews the OA results and prepares findings and recommendations. The updated package is then submitted to the ITIB.

[19] Appendix-D

5.3.6 Investment Decisions

The ITIB, after reviewing the OA and the recommendations of InvM, makes one of the following decisions:

1. Continue the investment "as is" and approve to move to the OA stage;
2. Recommend corrective actions – the ITIB may recommend corrective actions for the following:
   - Project performance variance exceeds ten (10) percent from the project's established baseline;
   - There are constant changes in the requirements and work scope;
   - A particular task on the critical path is missed with no alternative. This may include a major milestone or work product which was missed or delayed;
   - The investment's outcome does not adequately support the mission, business, or security function;
   - Major problems hinder the planned investment development.

   These recommendations are shared with the InvM for incorporation into the monthly submission to the DOI.
3. Rebaseline the investment. PMs, with sponsor concurrence and approval, may request ITIB approval to be re-baselined with new performance targets (scope, schedule, or budget performance goals). The sponsor, by requesting approval from the ITIB for a project re-baselining, is accepting the additional risk and management oversight responsibilities to ensure the investment is delivered within the revised project baseline.
4. Terminate the investment. If the above three options are not applicable or met by the investment, then the ITIB may terminate the investment.

5.3.7 Operation

The project is operational and is in the OA stage.

The formal monitoring of investment progress, and the determination of risks and returns, continues throughout the life of the investment or until the investment is enhanced. The investment is considered to be in O&M or Steady State (SS). The following activities may be performed without requiring a rebaseline or completion of an MNS.

- Technical Refresh (swapping out old hardware with newer hardware to perform the same function but improve performance);
- Upgrading/adding bandwidth capacity;
- Patch Management;
- Release Management (installing new releases of the same software vs. new/full versions);
- Cleanup of existing directories performance;
- Monitoring and Management of existing network;
- Replacing or moving an existing office circuit from one location to another;
- IT service and support to end users; and
- Replacing defective HW with a new unit that is fundamentally the same but without defect.

5.3.8 Capture Lessons Learned

The Evaluate Phase also provides the project sponsor and the PM with an opportunity to assess and share lessons learned about the CPIC management processes. The InvM uses these assessments to recommend CPIC process improvements to the ITIB

To capture "lessons learned," the project sponsor develops an investment management report and an Investment Evaluation Data Sheet (template is available on the BLM CPIC website[20]) and submits it to InvM. All failures and successes are collected and shared to ensure that future initiatives benefit from past experiences. A high-level assessment of management techniques, including organizational approaches, budgeting and acquisition, contracting strategies, tools and techniques, and testing methodologies is essential to establish realistic baselines and to ensure the future success of other IT initiatives.

5.4 Exit Criteria

Prior to exiting the Evaluate Phase, investments must have completed the following activities:

- Conducted a PIR;
- Established an OA review schedule.

Table 5-1 provides a summary of the documents generated during the Evaluate Phase process and if the document requires approval or is required only for filing and record keeping purposes.

Document	Required For File	Required For Approval
PIR Presentation	X	X
Updated Business Case	X	
Operational Analysis Schedule	X	
Operational Analysis	X	X

Table 5-1: Summary of documents generated during the Evaluate Phase

The investment remains in the OA stage until a decision is made by the BLM ITIB to modify, replace, or retire the system.

New development, modernization or major enhancements to OA systems are required to complete an MNS and start at the Pre-Select Phase. DME is the program cost for new IT investments, changes or modifications to existing systems to improve capability or performance, changes mandated by the Congress or agency leadership, personnel costs for IT investment and project management, and direct support. Examples of DME include:

[20] Appendix-D

- hanges to IT that impact the organizational and operational capabilities and/or existing business processes that may impact end-users;
- evelopment: the introduction of any new functionality or capabilities that do not currently exist whether internally owned and operated or outsourced to an external entity.
- odernization: migrations to new computing platforms, e.g. virtualization, cloud computing migrations where new skills, equipment and software may be needed to operate the application, system or infrastructure.
- nhancement: Upgrades to new versions of software (SW) including operating systems. Deployment of new hardware (HW) platforms, which are significantly different from current operational HW where new skills, equipment and software may be needed to operate the application, system or infrastructure.
- utfitting a brand new office with IT;
- mplementation of new performance monitoring tools; and
- ignificant efforts to consolidate circuits at co-located sites.

6 Waiver

6.1 Purpose

The waiver process provides a standardized guideline for requesting an exception to the process, procedure, and/or regulation, specifically as it relates to IT investments and associated funding. For example, a natural disaster may necessitate that the Pre-Select Phase or Select Phase be waived to expedite the IT Investment Management Process, or an appeal made to exceed approved funding levels. A mandated or unforeseen IT expenditure may result in the submission of a waiver request which would require modifications to the IT Spend Plan. However based on the nature of the investment, IT Security, Privacy, and EA screening procedures may have to be implemented as an out-of-cycle process. Upon approval, this change will be incorporated into the BLM's IT portfolio.

6.2 Entry Criteria

Prior to submitting a waiver, the request must meet one of following criteria:

- A BLM mission-critical system, infrastructure, or replacement resulting from an emergency condition;
- A mandated or unforeseen expenditure;
- The result of a Congressional directive that must be in place within a very short period of time;
- The result of a DOI directive that must be in place within a very short period of time.

6.3 Process

Figure 6-1 provides a summary of the waiver process as well as the individual(s) and/or group(s) responsible for completing each process step.

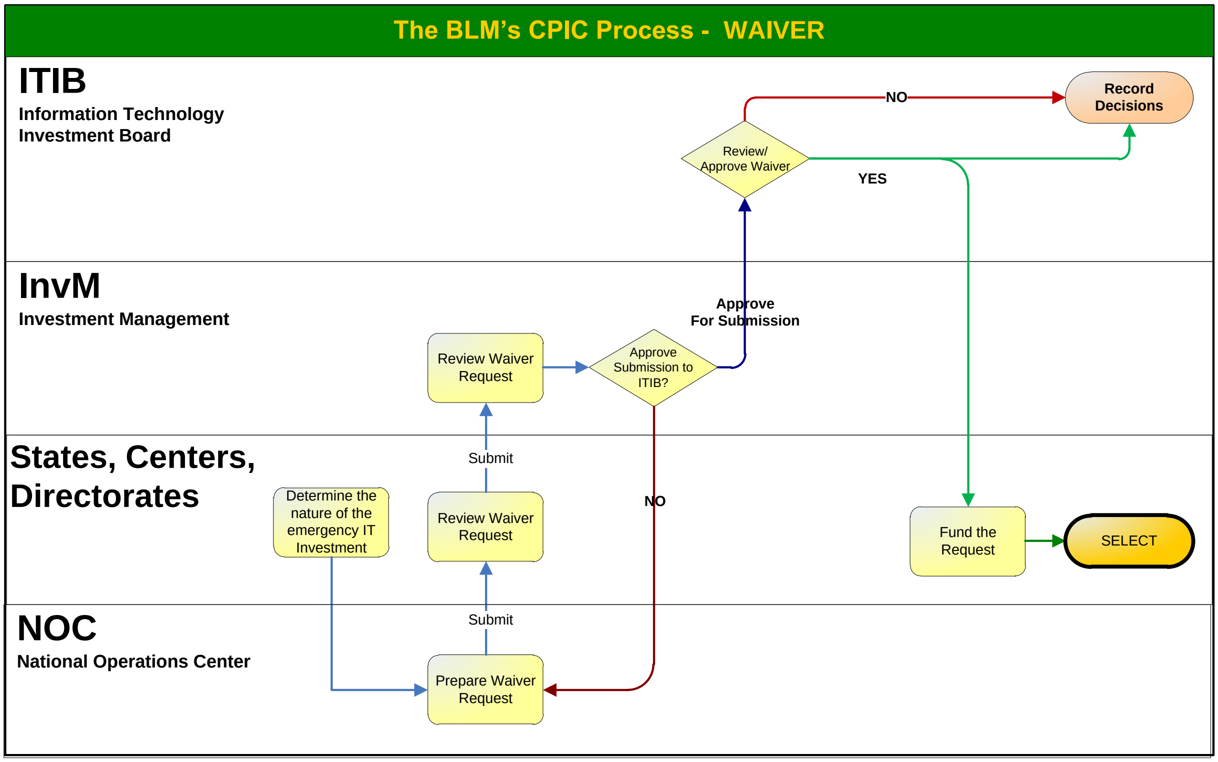

The BLM's CPIC Process - WAIVER
ITIB
Information Technology Investment Board
Record Decisions
NO
Review/ Approve Waiver
YES
InvM
Investment Management
Approve For Submission
Review Waiver Request
Approve Submission to ITIB?
States, Centers, Directorates
Submit
NO
Determine the nature of the emergency IT Investment
Review Waiver Request
Fund the Request
SELECT
NOC
National Operations Center
Submit
Prepare Waiver Request

Figure 6-1: Waiver Process

6.3.1 Determine the Nature of the Emergency IT Investment

The criteria defined in Section 6.2 may necessitate that the investment sponsor determines if an emergency waiver is appropriate.

The investment sponsor will work with the NOC to determine if an existing application/system may be able to meet the immediate requirements of the investment for which the emergency waiver is being developed. The investment sponsor will also work with the NOC to determine new or proposed hardware, software or service contract acquisition to meet the requirements of the waiver.

6.3.2 Prepare Waiver Request

The investment sponsor and the PM prepare a waiver request. The waiver request provides supporting justification as to why the waiver is being requested. The following are addressed:

- Nature and circumstances of the need;
- The scope of the new or proposed investment or new or proposed acquisition ;
- A proposed budget or spending plan;
- Description of risk and impact.

6.3.3 Submit Waiver Request

All completed waiver requests must be submitted to the InvM who will facilitate the expedited ITIB approval process.

6.3.4 Review Waiver Request

The waiver request is reviewed by the InvM to determine potential funding issues and conflicts, as well as describing the impacts to the total IT Portfolio. The InvM will also develop IT portfolio adjustment alternatives or strategy should the ITIB approve the exemption.

6.3.5 Decision for submitting Waiver Request

The InvM recommends the waiver to the ITIB. If it is concurred by the ITIB, it is forwarded to the BLM Deputy Director for approval. If it is rejected, it is returned to the investment sponsor.

6.3.6 Decision for Waiver Request

ITIB members analyze the information with findings and recommendations provided. This could be at a normally scheduled meeting, an emergency meeting, or a telephone/video conference. From this information, they will make their decision to exempt the investment from the specified process or not.

6.3.7 Fund the Request

Based on the nature and the alternatives presented, the ITIB decides to approve the investment or acquisition by adjusting the IT Portfolio. Approving the investment or acquisition will have an impact on the IT portfolio which will be documented by the InvM.

The Record of Decision is documented by the InvM and the investment re-enters the CPIC process.

6.4 Exit Criteria

The exception investment must obtain ITIB approval.

Table 6-1 provides a summary of the documents generated during the waiver process and if the document requires approval or is required only for filing and record keeping purposes.

Document	Required For File	Required For Approval
Waiver Request	X	X
Supporting Documents	X	

Table 6-1: Summary of documents generated during the waiver process

7 Portfolio Management

7.1 Purpose

The purpose of IT Portfolio Management is to ensure that an optimal mix of IT investments with manageable risk and returns is defined, selected, and funded. Portfolio Management comprises the following:

- Defining portfolio goals and objectives;

- Understanding, accepting, and balancing trade-offs;
- Identifying, eliminating, and minimizing risks;
- Monitoring and measuring portfolio performance;
- Assessing whether desired goals and objectives have been obtained and;
- Determining how each portfolio fits into the BLM's overarching architecture including IT Modernization Blueprints for key lines of business.

IT Portfolio Management delivers the following benefits:

- Contributes to investment management decision-making by providing pertinent information;
- Provides key information for monitoring cost and performance;
- Provides information for investment decisions throughout the life of the investment.

7.2 Pre-requisites

In order to perform the activities associated with selecting, funding, and managing an optimal IT investment portfolio, adequate resources must be provided for executing the process.

- ITIB members must exhibit core competencies in portfolio management.
- All investments within the portfolio must be analyzed and prioritized based on each investment's CSBR throughout the investment's lifecycle.
- BLM must have defined its common portfolio categories.

7.3 Process

The portfolio management process ensures that the ITIB collectively analyzes all investments and proposals to select those that best fit with BLM's strategic business direction, needs, and strategic vision. In addition, BLM has fiscal and workforce constraints that must be weighed against the risks and the long term return on investments within the portfolio. When making portfolio decisions, executives must consider use of IT resources along with work force and contracting options available to meet mission objectives.

To address these practical limits, portfolio management uses the following categories to aid in investment comparability and oversight.

- Part 1. IT Investments for Mission Delivery
- Part 2. IT Investments for Administrative Services and Support Systems
- Part 3. IT Investments for IT Infrastructure, IT Security, and IT Management

Starting FY2017 the OMB has restructured the IT Portfolio. The following table shows the mapping between the Old Parts, the New Parts and the nomenclature that BLM will be using for the Parts.

Old Part	New Part	BLM Nomenclature
Part 1. IT Investments for Mission Delivery Area and Management Support Area	**Part 1**. IT Investments for Mission Delivery	**Part 1**
	Part 2. IT Investments for Administrative Services and Support Systems	**Part 2**
Part 2. IT Investments for IT Infrastructure, IT Security,	**Part 3**. IT Investments for IT Infrastructure, IT Security, and IT	**Part 3A**

Office Automation, and Telecommunications	Management	
Part 3. IT Investments for EA, Capital Planning, and CIO Functions		**Part 3B**

Table 7-1: Mapping of Parts

Once all investments within the portfolio are categorized, investments and proposals can be compared to one another within and across portfolio categories, and the best overall portfolio can be selected and funded.

Each year, the BLM assesses its IT investment portfolio (section 7.4) to determine the optimal use of resources in the upcoming budget request. The BLM recommends a proposed portfolio to the DOI for review and analysis. The goal of this analysis is to ensure clear alignment between IT Portfolio, Department Strategic Plan, and Secretarial priorities. After DOI completes its review and makes any necessary adjustments, the DOI-CIO and the DOI's Director of Budget jointly certify the budget request, and DOI submits the DOI's full IT portfolio to the OMB.

During any FY, the BLM will complete the budget cycle for two years and include these costs in the budget submission. For example in FY 2016, the BLM will complete the BY 2017 budget cycle with Passback (President's Budget) submission to OMB, and continue planning for the BY 2018 budget cycle.

7.3.1 Portfolio Formulation

Throughout the FY, investments must complete the OMB and the DOI requirements as part of the budget cycle. The requirements and processes outlined in this section are to assess the costs and benefits of all proposed IT investments and to formulate the optimal portfolio of IT investments for the upcoming BY. Through this process, the BLM funds and prepares IT investments that best support the BLM's mission and strategic priorities for success.

During any FY, the BLM will complete the budget cycle for two years and include these costs in the budget submission. For example in FY 2016, the BLM will complete the BY 2017 budget cycle with Passback (President's Budget) submission to OMB, and continue planning for the BY 2018 budget cycle. Integration between budget and IT portfolio development occurs at three important submission periods as illustrated in the figure below. To clearly elaborate the budget cycle we have used FY2016 as an example while depicting the associated requirements for BY2017 and BY2018.

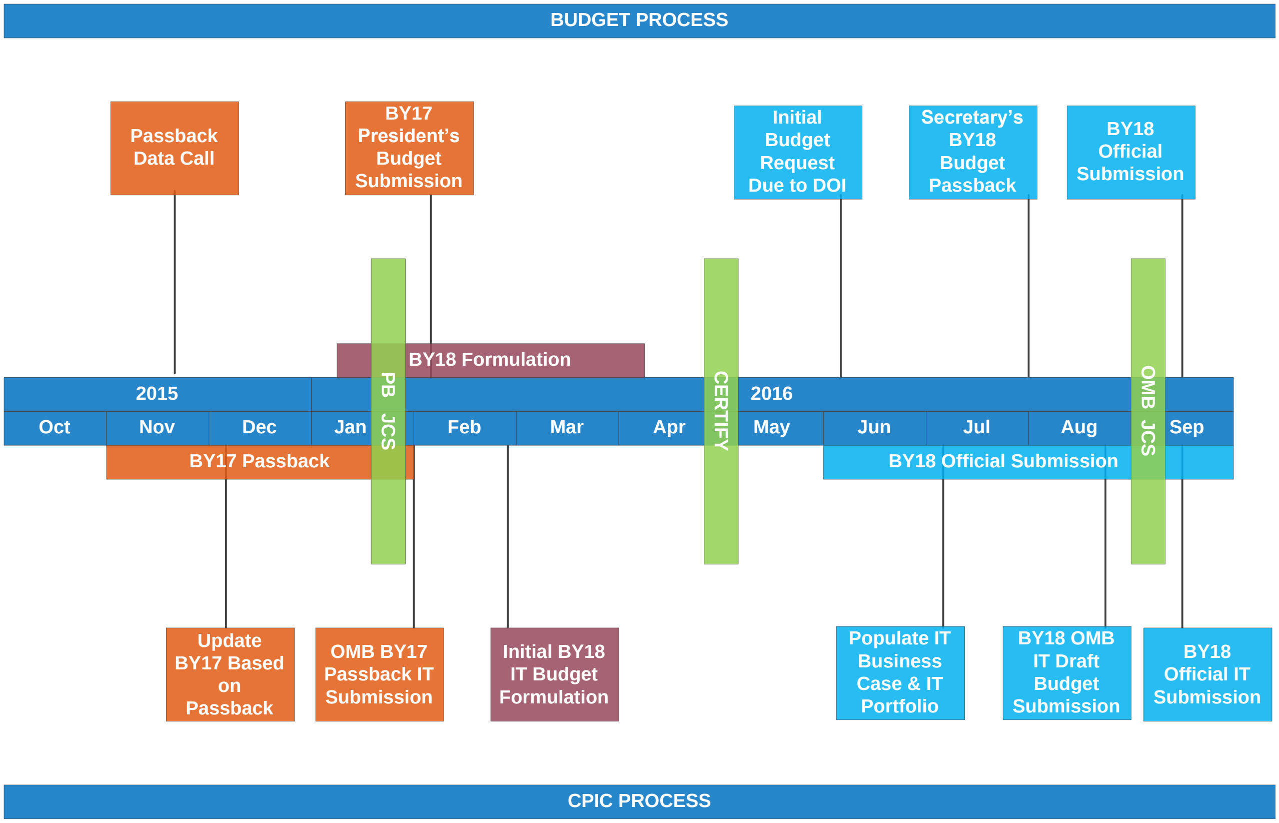

BUDGET PROCESS
Passback Data Call
BY17 President's Budget Submission
Initial Budget Request Due to DOI
Secretary's BY18 Budget Passback
BY18 Official Submission
BY18 Formulation
PB JCS
CERTIFY
OMB JCS
2015
2016
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
BY17 Passback
BY18 Official Submission
Update BY17 Based on Passback
OMB BY17 Passback IT Submission
Initial BY18 IT Budget Formulation
Populate IT Business Case & IT Portfolio
BY18 OMB IT Draft Budget Submission
BY18 Official IT Submission
CPIC PROCESS

Figure 7-1: Integration of Budget and CPIC Processes

Key milestones include:

- **BY 2017 Passback (President's Budget) IT Submission:** BY 2017 figures should be updated in the eCPIC system, the Department's IT portfolio management tool, to reflect the President's Budget (November/December). This is an official OMB requirement.
- **BY 2018 IT Budget Formulation**: BLM must reflect their BY 2018 funding recommendations in eCPIC (February/March). This is an internal Department requirement.
- **BY 2018 Official IT Budget Submission**: The Department's BY 2018 budget decisions are submitted to reflect Deputies Operation Group (DOG) and Principals Operating Group (POG), Working Capital Fund (WCF) costs, and Secretary's Passback decisions (July-September). This is an official OMB requirement.

7.3.2 IT Spend Plan

In order to accurately and collaboratively formulate the BLM's IT Portfolio, the Directorate of BFIRM issues the IT Spend Plan template to all investments and offices for completion and submission. The IT Spend Plan templates include detailed instructions for completion.

For investments that are in the Part 1 IT Investments for Mission Delivery and Management Support Portfolio:

- The Investment Manager shall use the IT Spend Plan templates to develop the initial draft Spend Plan for each investment.

- The Investment Manager should work with the PM from the NOC and the WO800 to recommend adjustments to the IT Spend Plan.
- The Investment Manager and the PM may ask for a one-on-one review session with the InvM during the development and prior to submission of their respective Spend Plan, as needed.
- The Investment Manager should submit the plan to their Investment Sponsor for approval. The submission should include a statement of certification that the submission has been reviewed by the PM, received concurrence and approved by the respective Budget Office (BO) and the Investment Sponsor.
- Once approved by the Investment Sponsor, the IT Spend Plan should be submitted to the InvM for review, analysis and submission to the ITIB for approval. The InvM may request additional information, clarifications, and justifications.
- Once approved by the ITIB, the final IT Spend Plan shall be incorporated into BLM's IT Portfolio and submitted to the DOI for approval and incorporation into the President's Budget.

For investments that are in the Part 3A and Part 3B IT portfolios:

- The Zone Chief shall use the IT Spend Plan templates to develop the initial draft Spend Plan for each States, Centers, and Directorates as per the needs of States, Centers, and Directorates then the States, Centers, and Directorates shall determine what they can afford. The NOC shall provide input into the assets that need to be refreshed.
- The Zone Chiefs should work with the SME from the NOC and the WO800 to recommend adjustments based on existing enterprise support and procurement plans for the IT Spend Plan.
- Once all comments have been compiled, the Zones Chiefs should submit the proposed plan to the States, Centers, and Directorates for review. The States, Centers, and Directorates should review the comments and work with the Zone Chiefs through negotiation until a consensus plan has been developed between all parties.
- The States, Centers, and Directorates may ask for a one-on-one review session with InvM and the Zone Chiefs during the development and prior to submission of their respective Spend Plan, as needed.
- The States, Centers, and Directorates should submit the plan to their State/CDs for approval. The submission should include a statement of certification that the submission has been reviewed by NOC Zone Chief, received concurrence and approved by the respective BO and Assistant/State/CDs.
- Once approved by State/CDs, the IT Spend Plan should be submitted to the InvM for review, analysis and submission to the ITIB for approval. The InvM may request additional information, clarifications, and justifications.
- Once approved by the ITIB, the final IT Spend Plan shall be incorporated into BLM's IT Portfolio and submitted to the DOI for approval and incorporation into the President's Budget.

The individual plans and actual spending will be monitored by the InvM during the FY.

IT Acquisitions Spend Plan

The BLM is required to develop and submit a comprehensive IT Acquisitions Spend Plan (ASP) to the DOI for review and approval. The IT ASP is generally due to the DOI in the First Quarter of each Fiscal Year. The DOI requires the BLM to report the following data in the IT ASP

- Item description
- Type of Product

- Count
- Category (Hardware, Software or Service Contract)
- Purpose of the Acquisition
- Estimated Cost
- ITT Product Service Type
- ITT Service Tower Type
- Offices supported
- Investment Name

The InvM uses the Part 1, Part 3A and Part 3B IT Spend Plans submitted by the offices to extract the data required to develop the BLM's IT ASP. After review and approval of the AD-BFIRM, the IT ASP is submitted to the DOI for review and approval by the CIO. Only after the DOI CIO has approved the BLM's IT ASP can the BLM offices procure items listed in the IT ASP.

7.3.3 FY Budget Cycle Requirements

In order to complete a successful budget submission to the DOI and OMB, the BLM must complete the following requirements throughout the FY:

- Ongoing IT Portfolio Review and Analysis;
- Budget Formulation Forms (BFF) for Part 1 (section 7.3.5);
- IT Portfolio Part 3 Workbooks;
- Portfolio Profiles;
- Joint Certification Statement;
- Agency IT Portfolio/Investment Updates; and
- Any additional requirements related to Enterprise-wide Investments;

To clearly elaborate the budget cycle we have used FY2016 as an example while depicting the associated requirements for BY2017 and BY2018. The requirements outlined above align with the key submission periods of the BY 2017 and BY 2018 budget cycles. Each falls within BY 2017 Passback (President's Budget), BY 2018 Formulation, and/or BY 2018 Official submission. As reference, the table below contains the components of each submission period.

	2015			2016								
	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep
Ongoing IT Portfolio Review/Analysis	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Budget Formulation Form				🟧	🟧							
Part 3 Workbook		🟥	🟥		🟧				🟦	🟦	🟦	
Portfolio Profiles			🟥			🟧					🟦	
Joint Certification Statement				🟥							🟦	
IT Portfolio / Business Case Update									🟦	🟦	🟦	
		BY 17 Passback Activities							BY 18 Submission Activities			
				BY 18 Formulation Activities								

Figure 7-2: Budget Cycle

7.3.4 Ongoing IT Portfolio Review and Analysis

The InvM must ensure that the BLM's portfolio contain all of BLMs IT investments. The InvM makes modifications to the BLM portfolios on behalf of Investment Sponsors. The BLM ITIB must approve the IT investments, in close coordination with the BLM Budget Officer and BLM Assistant CIO (ACIO). The InvM must populate the following three BLM portfolios within eCPIC:

- **Systems Portfolio (Systems)**: All Major and Non-Major investments including WCF investments. In relation to the IT Portfolio, this portfolio will consist of the BLM Part 1 IT Investments for Mission Delivery and Management Support Portfolio.
- **Infrastructure and Planning Portfolio (InfraPlanning)**: All BLM Part 3 IT Investments for Infrastructure, Office Automation, Telecommunications, EA, Capital Planning, and CIO Functions portfolios investments including WCF investments.
- **System Contribution Portfolio (SysContrib)**: This portfolio is for all contributions for Enterprise-wide systems. The Enterprise-wide investments within the DOI IT portfolio provide services to the BLM and include internal costs and/or WCF contributions. The DOI Enterprise Investment Manager collects and populates data into eCPIC for these investments. The BLM is responsible to review and address any questions or issues with the DOI Enterprise Investment Manager. This portfolio includes the following:
  - Consolidated business case contributions (e.g., FBMS, DOI Learn); and
  - System direct bill/variable IT investments (e.g., HRLoB).

7.3.5 IT Budget Formulation Forms for Part 1

The BLM must complete the IT BFF for all new and existing IT investments that are in the BLM Part 1 IT Investments for Mission Delivery and Management Support Portfolio. The purpose of this request is to provide the BLM with a tool to inform their initial select processes, and to provide the DOI with information on all IT investments to perform the business/technical fit analysis. The BFF questions cover

- basic IT investment information;
- IT investment funding levels;
- customer satisfaction;
- strategic/mission alignment; and
- technical currency.

7.3.6 IT Portfolio Part 3 Workbooks

The BLM must update their Part 3 internal IT investment costs and provide an "explanation of change" using the Microsoft Excel workbooks provided by the DOI. The BLM is required to fill in an Explanation of Change (EOC) for any change to their internal costs for PY, BY and CY. This information enables the DOI to understand why the total funding amounts for the BLM change. The DOI combines BLM's Part 3 internal IT investment costs with the BLM's WCF contributions to the same IT investments, as applicable, and uploads both into the eCPIC to populate the funding tables. This process ensures consistency and accuracy of the WCF budget data at a point in time.

The Joint Certification Statement (JCS), signed by the BLM ACIO and the BLM BO, includes the costs entered into these workbooks. Prior to submission of the BLM Part 3 internal IT investment cost data to the DOI, the BLM must coordinate the internal funding entered in these workbooks with the BLM ACIO and the BLM BO, as they must confirm these numbers before any submission to the DOI.

The BLM should review its portfolio on an ongoing basis. When the BLM determines that an IT component is not being reported, or when IT is no longer used, IT investments should be added or removed, respectively, from one of the above portfolios. Both the BLM ACIO and the BLM BO should be notified and consulted as changes are made to the BLM IT portfolio. In addition to accurately placing IT investments within the correct portfolios, it is also essential that the BLM accurately and consistently categorize IT spending.

7.3.7 Portfolio Profiles

The Portfolio Profile is a tool developed by the DOI to summarize and document internal and OMB submissions. It is comprised of four sections; Submission Comparison Overview, Submission Comparison EOC, BY Overview, and BY EOC and More Accurate Reporting (MAR). Listed in the below table is a description of each section.

Section	Description
Submission Comparison Overview	• This section provides a comparison of the different versions of the BLM’s IT Portfolio between the current submission period and the previous submission period (i.e. During Official submission it will compare against Formulation). • The BLM must provide an EOC for any differences in the total count of major IT investments, non-major IT investments, and Contribution IT Investments.
Submission Comparison EOC	• This section provides a comparison between the prior year (PY), current year (CY), and BY between submissions (i.e. It will compare “Total FY 2015 Agency Funding from BY 2017 Formulation” with “Total FY 2015 Agency Funding from BY 2017 Official”) • The BLM must provide an EOC for funding differences between submissions.
BY Overview	• This section provides a comparison between the counts of IT investments year-to-year. • The BLM must provide an EOC for any differences year-to-year.
BY EOC and MAR	• This section compares the agency funding amounts year-to-year. (i.e. Compares funding amounts for 2015, 2016, and 2017 and shows a delta where funding has changed) • The BLM must provide an EOC for any differences in funding between years. • This section also allows the BLM to explain that funding increases or decreases are due to MAR (i.e. reporting costs that were previously misreported as non-IT, or removing costs that are non-IT)

Table 7-2: Portfolio Profiles

7.3.8 Joint Certification Statement

In response to the OMB requirements outlined in FITARA, the DOI initiated a joint certification process where the DOI certify the IT Portfolio prior to any submission to the OMB. First, the BLM BO and the BLM ACIO must jointly sign the JCS to certify prioritization and allocation of IT investment costs. Once signed at the BLM level, the DOI CIO and the Director of Budget will certify the entire request and submit a JCS Budget Exhibit to the OMB. The DOI will distribute the JCS to the BLM twice during a FY, once during BY Passback (President's Budget) and once during BY Official submission. It will consist of the following components:

- JCS Budget Exhibit:
  - Crosswalks IT investment funding data from eCPIC, Budget Formulation, Budget Execution and WCF and identifies PY, CY and BY funded amounts per IT investment title for the BLM;
  - Is a macro-enabled MS Excel workbook, used to simplify data entry and minimize workload.
- JCS Signature Page:
  - Was created in response to the FITARA statute and meets requirement for the CFO (i.e. POB) and the CIO to communicate on IT portfolio priorities;
  - Adheres to OMB A-11 guidance requiring CIO to approve, POB to support , and IT Capital Planning Office to coordinate/review; and
  - Requires BBO and ACIO signature.

While coordinating BY Passback (President's Budget) and BY Official submission IT budget needs with the BLM budgets, the BLM ACIO and the BLM BO should review the IT Portfolio Summary to ensure alignment with BLM operating plans and the Congressional Justification.

7.3.9 IT Portfolio/Investment Updates

All Major and Non-Major Mission IT investments must update the IT Portfolio Summary information in eCPIC prior to the BY official IT budget submission. The BLM ITIB and the BLM ACIO must review the BY budget requests. Prior to the submission the BLM BOs should validate the submission to ensure each IT investment's life cycle costs table, funding sources, and FTE tables match bureau or office funding for PY, CY, and BY.

Using FY2016 as an example, funding for PY, CY, and BY represents the following:

- PY 2016: The actual dollar amount spent in FY 2016 attributed to this investment. This includes carry-over money from past years.
- CY 2017: The funding amounts approved in the enacted BY 2017 President's Budget. Ideally, this amount will not change between BY 2017 Passback (President's Budget) submission and BY 2018 Official submission.
- BY 2018: The requested funding for FY 2018. This includes funding requested for new initiatives, as well as funding to maintain current operations.

Additionally, all Major IT investments should update both the Major IT Business Case and the Major IT Business Case Detail processes in the eCPIC. The Major Investment Business Cases provide the budgetary and management information necessary for sound planning, management, and governance of IT investments. These documents help the BLM explicitly align IT investments with strategic and performance goals, and ultimately provide value to the public by making IT investment and management information more transparent.

7.4 Portfolio Evaluation

Portfolio evaluation focuses on the assessment of the overall health and performance of the IT Portfolio. Portfolio and project reviews are conducted to provide for the assessment and to make necessary adjustments to the IT Portfolio. The BLM uses the BLM Status (bStat) process (section 7.4.1) and Rating and Ranking process (section 7.4.2) to conduct the evaluation of the IT Portfolio.

After examining all IT assets in light of the BLM's business objectives and assumptions, the ITIB prioritizes business objectives and then evaluates proposed IT Investments against those objectives using enterprise portfolio analysis software tools. Upon approval of the outcome, the ITIB conducts portfolio optimization to determine the best mix of investments, thus helping to align resources behind the most effective means of achieving Agency objectives.

7.4.1 bStat

The bStat is face-to-face, evidence-based accountability review of an IT investment with BLM's leadership. The purpose of the bStat is to control and evaluate the results of IT investments and to result in concrete actions to address weaknesses. The bStat reduces wasteful spending by turning around troubled programs and terminating failed programs sooner.

bStat is

- **Actionable**: participants should leave the session armed with next steps to improve outcomes
- **A Spotlight**: sessions should highlight problems areas and focus deeply on pain points
- **Prescriptive**: sessions should result in clear actions, with owners and deadlines
- **A Tool**: sessions should be used when executive level influence is needed

bStat is not

- **Routine**: sessions should not be used for routine, small impact change requests
- **Comprehensive**: not an IV&V, IBR, PIR (though these could be inputs or requested actions of a bStat)
- **One-Size-Fits-All**: will need to be customized for investments of varying size and complexity
- **A Review**: sessions should not be used for cyclical control reviews ("business as usual")

The bStat process consists of the following steps which are managed by the InvM.

1. Discovery
    a. Identify Investment for Review
    b. Notify Investment Manager and Business Owner
2. Analysis
    a. Collect Investment Artifacts
    b. Engage SMEs
    c. Formulate Thesis, Validate Facts and Synthesize Analysis
3. Preparation
    a. Invite Attendees
    b. Prepare Executive Briefing
    c. Complete Administrative and Logistics Support
    d. Pre-Brief AD-BFIRM
4. Facilitation

   a. Conduct bStat session
   b. Record Action Items with Owners and Timelines
5. Follow-up
   a. Distribute Memo of Record
   b. Enter and Track Action Items to Conclusion in Repository
   c. Incorporate Lessons Learned in Enterprise

Table 7.3 lists the roles and responsibilities of bStat participants.

Roles & Responsibility	InvM	Project Management	Business Owner	ITIB
Identify investments for bStat	Primary			X
Lead the documentation review, perform critical analysis, and provide briefing materials to the IRB prior to the meeting	Primary			
Support documentation review	Primary			X
Track and monitor action items resulting from bStat	Primary			
Brief leadership prior to the meeting	Primary	X	X	
Provide full and complete documentation to support a given review		Primary	X	
Execute Action Plan resulting from bStat Reviews		Primary	X	
Present findings to ITIB	Primary	X		
Coordinate and facilitate bStat meeting	Primary			
Lead bStat meeting and ask probing questions				Primary
Provide expert advice and objective recommendations that assist the ITIB in decision-making	X			
Notify Investment of bStat	Primary			
Document decisions and action plan resulting from bStat	Primary			
Attend bStat and contribute to group decisions	X	X	X	X

Table 7-3: bStat Roles and Responsibility

bStat results in one or more of the following outcomes:

- Continue as planned with minor recovery and corrective action plans;
- Continue with modifications such as:
  - Rescope and rebaseline,
  - Reassess make/buy approach,
  - Reassign project team and/or vendor,
  - Implement extensive corrective action plans,
  - Thorough root cause analysis of performance issues;
- Halt investment and:
  - Determine if the project is still necessary,
  - Recharter –performs a deeper analysis of the program,
  - Stabilize the application to a point of non-impact to users and business operations.
- Action Items
- Lessons Learned

7.4.2 Rating & Ranking

The performance of BLM's entire IT Portfolio is reviewed throughout the year by InvM. In practice, the BLM IT Portfolio evaluation process provides the basis to re-affirm or "re-select" funded projects on the basis of continuing to meet a business need and meeting project performance objectives, such as cost, schedule, and technical performance. In order to create an optimized portfolio, it is vital that all IT investments have been uniformly judged on both their merits and liabilities.

The ITIB uses Rating and Ranking Criteria (available on the BLM CPIC website[21]) to score investments. The ITIB reviews each investment for compliance with BLM's strategic, legislative, and budgetary goals and evaluates the investment based on established rating and ranking criteria. The result of the bStat process is used to facilitate the Rating and Ranking of investments.

The ITIB has appointed the RRC to review and assess the health of all BLM IT Investments, and to make recommendations for further improvement. RRC will rate and rank the BLM IT Investments in accordance with the Rating and Ranking Criteria established by the ITIB.

The scope of the RRC is all BLM IT Investments, including:

- Major Investments that are in Part-1 of BLM's Exhibit 53
- Non-Major Investments that are in Part-1 of BLM's Exhibit 53
- Infrastructure Investments that are in Part-3 of BLM's Exhibit 53
- WCF Bills, and
- New Investments

The Rating and Ranking process is depicted in Figure 7.3 and described below.

A. Update Rating & Ranking Criteria Based on Latest Guidance from OMB/DOI (InvM) – Depending on the needs of the government or the agency, certain criteria might become more important in a given year or change entirely. The Rating & Ranking Criteria should be adjusted accordingly.
B. Present Updates for ITIB Approval (InvM) – InvM answers any questions the ITIB has regarding the OMB/DOI updates before ITIB votes whether to accept the updates as presented.

[21] Appendix-D

C. Approve (ITIB) – If ITIB approves the updates as presented the process may continue; otherwise ITIB must adjust the updates to better fit BLM's needs.

D. Prepare Investment Profile (Project Manager) – The PM for each investment completes/updates the IP.

E. Define Criteria of Value (ITIB) – Select the criteria that will be used to determine if a project successfully meets its goals. Describe each criterion so that each one can be measured across all investments.

F. Define Sub-criteria of Value (if necessary) (ITIB) – Initial criteria may be too broad; breaking them up into smaller criteria can help pinpoint the values most necessary to BLM.

G. Define Criteria of Risk (ITIB) – Select the criteria that will be used to determine the increased uncertainty and effort required by implementing/maintaining the investment. Describe each criterion so that each one can be measured across all investments.

H. Define Sub-criteria of Risk (if necessary) (ITIB) – Initial criteria may be too broad; breaking them up into smaller criteria can help pinpoint the liabilities BLM most wishes to avoid.

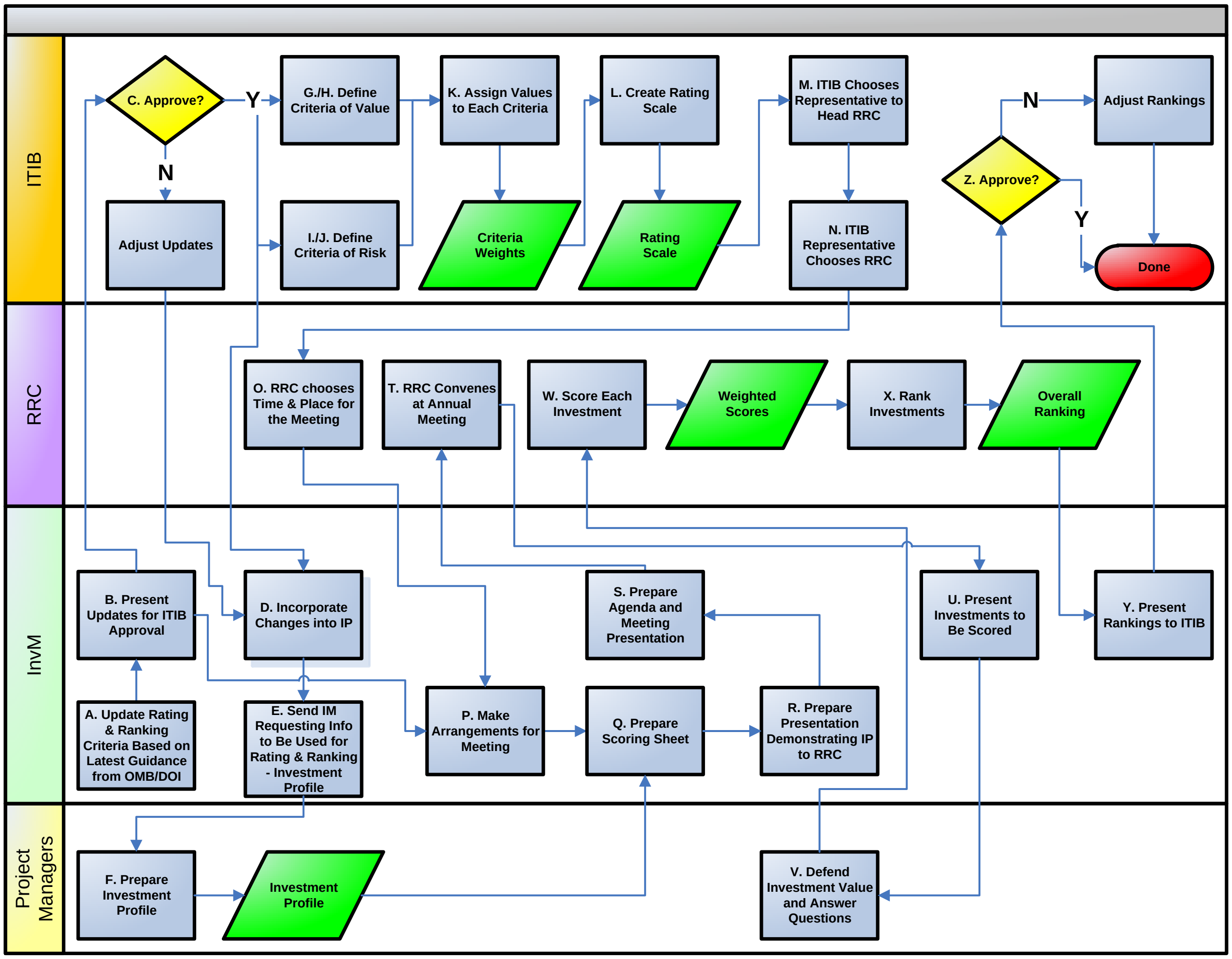

ITIB
RRC
InvM
Project Managers
C. Approve?
Y
N
Adjust Updates
G./H. Define Criteria of Value
I./J. Define Criteria of Risk
K. Assign Values to Each Criteria
Criteria Weights
L. Create Rating Scale
Rating Scale
M. ITIB Chooses Representative to Head RRC
N. ITIB Representative Chooses RRC
Z. Approve?
N
Y
Adjust Rankings
Done
O. RRC chooses Time & Place for the Meeting
T. RRC Convenes at Annual Meeting
W. Score Each Investment
Weighted Scores
X. Rank Investments
Overall Ranking
B. Present Updates for ITIB Approval
D. Incorporate Changes into IP
S. Prepare Agenda and Meeting Presentation
U. Present Investments to Be Scored
Y. Present Rankings to ITIB
A. Update Rating & Ranking Criteria Based on Latest Guidance from OMB/DOI
E. Send IM Requesting Info to Be Used for Rating & Ranking - Investment Profile
P. Make Arrangements for Meeting
Q. Prepare Scoring Sheet
R. Prepare Presentation Demonstrating IP to RRC
F. Prepare Investment Profile
Investment Profile
V. Defend Investment Value and Answer Questions

Figure 7-3 Rating and Ranking Process

I. Assign Values to Each Criteria (ITIB) – Determine how important each Criteria (and Sub-criteria, if necessary) is relative to the others. This will give the proper weight to each criteria and illuminate BLM's priorities.

J. Create Rating Scale (ITIB) – Determine the size of the scale (3-point scale, 7-point scale, etc.) and then define the meaning of each number on the scale.

K. ITIB Chooses Representative to Head RRC (ITIB) – This representative is charged with forming the team that will rate and rank the investments.

L. ITIB Representative Chooses RRC (ITIB) – This team should be a cross-section of the BLM.

M. RRC Chooses Time and Place for the Meeting (RRC) – The team members need to be in the same room when discussing the investments to ensure maximum cooperation and understanding.

N. InvM Makes Arrangements for Meeting (InvM) – This includes hotel accommodations, rental cars and plane flights (if necessary).

O. Prepare Scoring Sheet (InvM) – Because the RRC circles the scores they give each investment as they are presented, InvM creates the sheets needed to complete this exercise.

P. Prepare Presentation Demonstrating IP to RRC (InvM) – The IP does not match the Rating & Ranking questions on a 1:1 basis, but the presentation correlates the sections of the IP to the questions presented in Rating & Ranking.

Q. Prepare Agenda and Presentation (InvM) – InvM creates a slide deck that outlines the agenda and gives a briefing on the process and goals of the meeting.

R. RRC Convenes at Annual Meeting (RRC) – The meeting will last multiple days as major investments are likely to generate a great deal of discussion.

S. Present Investments to Be Scored (InvM) – InvM facilitates the meeting and makes any necessary adjustments to the agenda. The InvM representative is also responsible for ensuring the meeting moves along and finishes within the allotted time.

T. Defend Investment Value and Answer Questions (Project Managers) – PMs receive questions from the Rating & Ranking Team to clarify the value their projects bring to the agency. This can be done either in person or over the phone if the PM is unable to physically attend the meeting.

U. Score Investments (Rating & Ranking Team) – For each investment, assign point values from the Rating Scale for each Criteria and Sub-Criteria.

V. Rank Investments (RRC) – Using the weighted scores, rank the investments from most desirable to least desirable.

W. Present Rankings to ITIB (InvM) – Once the Overall Ranking has been confirmed by the Rating & Ranking Team, InvM presents the rankings and answers any questions the ITIB has.

X. Approve (ITIB) – ITIB votes whether to approve the list after InvM's presentation. If it does not approve the list it is tasked with rearranging the investments as it sees fit; otherwise the list stands and becomes the new prioritization for the FY.

7.4.3 PortfolioStat

The PortfolioStat is a tool that the DOI and the OMB use to assess the current maturity of their IT portfolio management process, make decisions on eliminating duplication, augment current CIO-led capital planning and IT investment control processes and move to shared solutions in order to maximize the return on IT investments across the portfolio[22]. In March 2012, the OMB established PortfolioStat accountability sessions, engaging directly with agency leadership to assess the effectiveness of current IT management practices and address opportunities to improve management of IT resources. The DOI

[22] Appendix-C

continues to need the BLM's participation to comply with OMB's PortfolioStat process. The OMB places a high importance on the PortfolioStat analysis across Federal agencies, and the DOI has committed to mature its PortfolioStat process. To support this effort, the DOI conducts quarterly PortfolioStat meetings with the BLM to assess their compliance with the FITARA[22].

The IDC is a component of the PortfolioStat. The IDC reports progress in meeting IT strategic goals and objectives as well as cost savings and avoidances resulting from implementing IT transition plans. The OMB established an IDC channel for agencies to report structured information. The BLM uses this channel to report the BLM's progress in meeting IT strategic goals, objectives and metrics as well as cost savings and avoidances resulting from IT management actions on a quarterly basis.

As part of the PortfolioStat, the data and input collected from the BLM consists of the following areas:

- **Inventory of Mobile Devices and Wireless Service Contracts**: The BLM must provide data for all wireless service contracts and supported mobile device hardware (mobile phones, tablets, and air cards) within the agency.
- **Cost Savings/Avoidance Decisions**: The BLM must report IT cost savings and avoidance strategies, realized amounts, and reinvestment plans for the funding as part of the IDC.
- **Open Data**: The BLM must create and maintain an Enterprise Data Inventory for the following:
    - Public Data Listing;
    - Process to engage with customers to help facilitate and prioritize data release;
    - Document if data cannot be released; and
    - Roles and responsibilities for promoting efficient and effective data release.

7.4.4 Quarterly IT Organizational Assessments

The DOI uses the FY OCIO Organizational Assessment to identify the BLM's FY quarterly ratings. The following Organizational Assessment Criteria is used by the DOI to assess the BLM in the Goal Area to Maximize the Value of IT Investments Metrics. The following six metrics are used by the DOI to determine the BLM's overall status rating in the Goal Area "Maximize the Value of IT Investments" For each of the six metrics, a maximum score of five can be obtained. These six scores are totaled to derive the BLM's Overall Status Rating for the quarter.

1. Increase the number of FAC-P/PM certified PM assigned to major IT Investments. The purpose of the FAC-P/PM is to establish general training, experience, and development requirements for program and PMs in civilian agencies based upon core competencies needed to successfully manage programs and projects. This certification program promotes continued development of essential knowledge and skills for PMs to improve program outcomes. Program and PMs of major investments and projects must attain FAC P/PM certification within one year from date of assignment to the project.
2. Increase Major IT investment compliance with OMB/OCIO project management artifact requirements. The OMB requires Major IT investments to develop, maintain, and submit the investment documents and artifacts listed in table 7-4. The BLM should provide updated versions (including date of last update) as significant changes are made or as available throughout the investment's lifecycle.

Artifact	Submission Frequency
Investment Charter, including the IPT (if/when projects are added to the investment, Investment	Submit once, update as needed.

charter should be updated).	
Investment-Level Alternative Analysis and Benefit-Cost Analysis	Submitted at least 2.5 years in advance of contract expiration or at minimum every 3 years once operational.
Risk Management Plan	Every two years.
Operational Analyses (for operational or mixed life cycle systems).	Annually for Major investments and every other year for Non-Major investments.
PIR Results (investment level or project specific).	As necessary within 6 months after implementation.
Documentation of Investment Rebaseline and Management	As applicable.
Acquisition Plan	Annually.

Table 7-4 Required Artifacts

3. Increase strong Major IT investment management execution to ensure IT investments are effectively managing cost, schedule, and performance. Major investments should be reporting against a current Investment Performance Baseline that is reflective of budget decisions, and is reflective of the full planned lifecycle. Once a current baseline has been established, EVM data can be monitored to ensure that an investment is meeting expectations of both cost and schedule. If an investment falls outside of the acceptable +/- 10% cost or SV, a CAR should be submitted.
4. Increase the % of Agency IT Portfolio Summary investments within the Bureau and Office portfolio that have applications associated with them. The Application Inventory metric supports the DOI’s continued effort to establish an enterprise-wide inventory of applications mapped to the DOI IT investment portfolio. The purpose of this effort is to establish a portfolio hierarchy, linking applications and investments which will enable a more accurate baseline of our IT spending, to gain a better understanding of the functional and technical profile of our investments, and inform IT decision-making.
5. Increase the % of bureau and office systems documented in the Cyber Security Assessment & Management (CSAM) tool that are mapped to IT investments. The CSAM rating is comprised of one element which is required to be completed in CSAM in order to be compliant. It is the correct investment UII code which should be mapped to the appropriate system name within CSAM. This rating will be assessed on a quarterly basis by running a report from CSAM to verify that all active bureau/office systems are mapped appropriately to a valid UII code.
6. Increase the % of all required fields populated within the Portfolio Profiles during BY Passback, BY Formulation, and BY Official Submission. The Portfolio Profile is a tool developed by the DOI to summarize and document internal and OMB submissions.

Appendix A - Definitions

Accessibility: Information technology products or services that are in full compliance with the standards of section 508 of the Rehabilitation Act of 1973.

Acquisition Plan: Description of the acquisition approach including:

- Contract strategy (definition of government and contractor roles and responsibilities);
- Use of COTS software;
- Major milestones (such as software releases, hardware delivery, installation, and testing).

Adequate security: Security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.

Agency: Any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any independent regulatory agency.

Agency Strategic Plan: A plan that provides general and long-term goals that the agency aims to achieve, the actions the agency will take to realize those goals, the strategies planned, how the agency will deal with challenges and risks that may hinder achieving results, and the approaches it will use to monitor its progress.

Agile Development: A development methodology that uses an iterative approach to deliver solutions incrementally through close collaboration and frequent reassessment.

Appropriations: An appropriation provides budget authority that permits Government officials to incur obligations that result in immediate or future outlays of Government funds. Regular annual appropriations are:

- Enacted normally in the current year;
- Scored entirely in the budget year; and
- Available for obligation in the budget year and subsequent years if specified in the language (see "Availability," below).

Architectural Alignment: Degree to which the IT initiative is compliant with the DOI's IT architecture.

Architecture: An integrated framework for evolving or maintaining existing technologies and acquiring new technologies to support the mission(s).

Assets: Tangible or intangible items owned by the Federal Government which would have probable economic benefits that can be obtained or controlled by a Federal entity.

Authorization to Operate (ATO): The official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.

Authorization boundary: All components of an information system to be authorized for operation by an authorizing official. This excludes separately authorized systems to which the information system is connected.

Authorization package: The essential information that an authorizing official uses to determine whether to authorize the operation of an information system or the use of a designated set of common controls. At a minimum, the authorization package includes the information system security plan, privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones.

Authorizing official: A senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation.

Availability: Appropriations made in appropriations acts are available for obligation only in the budget year unless the language specifies that an appropriation is available for a longer period. If the language specifies that the funds are to remain available until the end of a certain year beyond the budget year, the availability is said to be "multi-year." If the language specifies that the funds are to remain available until expended, the availability is said to be "no-year." Appropriations for major procurements and construction projects are typically made available for multiple years or until expended.

Baseline Goals: Baseline cost, schedule, and performance goals will be the standard against which actual work is measured. They will be the basis for the annual report to the Congress required by FASA Title V on variances of 10 percent or more from cost and schedule goals and any deviation from performance goals.
The goals, and any changes to the goals, must be approved by the OMB.

- Cost and schedule goals. The baseline cost and schedule goals should be realistic projections of total cost, total time to complete the project, and interim cost and schedule goals. The interim cost and schedule goals should be based on the value of work performed or a comparable concept.
- Performance goals. A target level of performance against which actual achievement or progress can be compared, preferably expressed as a tangible, measurable objective or as a quantitative standard, value, or rate. This can include goals containing key milestones or goals framed as a position relative to the past or relative to peers.
- Illustrative major milestones in establishing goals. Illustrative major milestones in establishing or proposing revised baseline goals could be:
  - Agency mission analysis, process design, and requirements development;
  - Agency submission and justification to the OMB;
  - Approval for inclusion in the Administration's budget proposal to the Congress;
  - Enactment of appropriations;
  - Before and after the contract or contracts are signed; and
  - Other times after the contracts are signed, depending on circumstances.

Benefit: Quantifiable or non-quantifiable advantage, profit, or gain.

Binding Operational Directive: A compulsory direction from the Department of Homeland Security to an agency that is for the purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk; shall be in accordance with policies, principles, standards, and guidelines issued by the Director of the Office of Management and Budget; and may be revised or repealed by the Director if the direction issued on behalf of the Director is not in accordance with policies and principles developed by the Director.

Budget Authority: The authority provided by law to incur financial obligations that will result in outlays. The specific forms of budget authority are appropriations, borrowing authority, contract authority, and spending authority from offsetting collections. This definition is the same as the one contained in section 3(2) of the Congressional Budget and Impoundment Control Act of 1974, which the Congress uses in the congressional budget process.

Budget Classification Categories: The Life Cycle Costs table in eCPIC, which feeds the Department IT Portfolio and Major IT Business Cases, collects funding at a detailed level of categories listed below:

- Government full time equivalents (FTE);
- Contract Services;
- Hardware Costs (HW);
- Software Costs (SW);
- Travel Costs;
- Rent, Communications, Utilities; and
- Other costs.

Budget Cycle: The overall estimated cost for one fiscal year including direct and indirect costs.

Budget Resources: Budget resources refer to the mean amounts available to incur obligations in a given year. Budgetary resources consist of new budget authority and unobligated balances of budget authority provided in previous years.

Business Case: Structured proposal for business improvement that functions as a decision package for organizational decision-makers. A business case includes an analysis of business process performance and associated needs or problems, proposed alternative solutions, assumptions, constraints, and risk-adjusted CBA. The business case is this document is for the DOI purposes.

Business Continuity Plan: A plan that focuses on sustaining an organization's mission or business processes during and after a disruption, and may be written for mission or business processes within a single business unit or may address the entire organization's processes.

Business Process: A collection of related, structured activities or chain of events that produce a specific service or product for a particular customer or group of customers.

Business Process Reengineering: A systematic, disciplined approach to improving business processes that critically examines, rethinks, and redesigns mission delivery processes.

Business Requirements Analysis: Identifies how personnel conduct business activities to fulfill mission requirements, meet objectives, and perform tactical plans.

Capital Asset: Tangible property including durable goods, equipment, buildings, installations, and land.

Certification and Accreditation: The official management decision given by a senior Agency official to authorize operation of an information system and to explicitly accept the risk to Agency operations, Agency assets, or individuals based on the implementation of an agreed-upon set of security controls.

Chief Information Officer: The senior official that provides advice and other assistance to the head of the agency and other senior management personnel of the agency to ensure that IT is acquired and information resources are managed for the agency in a manner that achieves the agency's strategic goals and information resources management goals; and is responsible for ensuring agency compliance with, and prompt, efficient, and effective implementation of, the information policies and information resources management responsibilities, including the reduction of information collection burdens on the public.

Chief Information Officers Council: The Council codified in the E-Government Act of 2002.

Commercially Available Off-The-Shelf (COTS) Item: Any item, other than real property, that is of a type customarily used by the general public for nongovernmental purposes, and that has been sold, leased, or licensed to the general public; is sold, leased, or licensed in substantial quantities in the commercial marketplace; and is offered to the Government, without modification, in the same form in which it is sold, leased, or licensed in the commercial marketplace.

Common control: A security or privacy control that is inherited by multiple information systems or programs.

Control Phase: Capital planning phase that requires ongoing monitoring of IT investments against schedules, budgets, and performance measures.

Controlled Unclassified Information: Information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended.

Cost: Defined in Statements of Federal Financial Accounting Concepts (SFFAC) No. 1, Objectives of Federal Financial Reporting, as the monetary value of resources used. Defined more specifically in Statements of Federal Financial Accounting Standards (SFFAS) No. 4, Managerial Cost Accounting Concepts and Standards for the Federal Government, as the monetary value of resources used or sacrificed or liabilities incurred to achieve an objective, such as to acquire or produce a good or to perform an activity or service. Depending on the nature of the transaction, cost may be charged to operations immediately (i.e., recognized as an expense of the period) or to an asset account for recognition as an expense of subsequent periods. In most contexts within SFFAS No. 7, Accounting for Revenue and Other Financing Sources, "cost" is used synonymously with expense.

Critical infrastructure: Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health safety, or any combination of those matters.

Customer: Groups or individuals who have a business relationship with the organization; those who receive or use or are directly affected by the products and services of the organization.

Cybersecurity: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation.

Development Modernization and Enhancement (DME): Per OMB, DME is the program cost for new IT investments, changes or modifications to existing systems to improve capability or performance, changes mandated by the Congress or agency leadership, personnel costs for IT investment and project management, and direct support. For major IT investments, this amount should equal the sum of amounts reported for planning and acquisition plus the associated FTE costs reported in the Major IT Business Cases. Examples of DME include:

- Changes to IT that impact the organizational and operational capabilities and/or existing business processes that may impact end-users;
- Development: the introduction of any new functionality or capabilities that do not currently exist whether internally owned and operated or outsourced to an external entity.
- Modernization: migrations to new computing platforms, e.g. virtualization, cloud computing migrations where new skills, equipment and software may be needed to operate the application, system or infrastructure.
- Enhancement: Upgrades to new versions of software (SW) including operating systems. Deployment of new hardware (HW) platforms, which are significantly different from current operational HW where new skills, equipment and software may be needed to operate the application, system or infrastructure;
- Outfitting a brand new office with IT;
- Implementation of new performance monitoring tools; and
- Significant efforts to consolidate circuits at co-located sites.

Discount Rate: The interest rate used in calculating the present value of expected yearly benefits and costs.

Dissemination: The government-initiated distribution of information to a nongovernment entity, including the public. The term 'dissemination,' as used within this Circular, does not include distribution limited to Federal Government employees, intra- or interagency use or sharing of Federal information, and responses to requests for agency records under the Freedom of Information Act or the Privacy Act.

Earned Value Analysis: A structured approach to project management and forecasting including comparisons of actual and planned costs, work performed, and schedule.

Efficiency measures: While outcome measures provide valuable insight into program achievement, more of an outcome can be achieved with the same resources if an effective program increases its efficiency. Agencies are encouraged to develop efficiency measures. Efficiency gains may be described as maintaining a level of performance at a lower cost, improving performance levels at a lower cost, improving performance levels at the same cost, or improving performance levels to a much greater degree than costs are increased. Simply put, efficiency is the ratio of the outcome or output to the input of any program.

Enterprise architecture: Means:

○

strategic information asset base, which defines the mission;

○

he information necessary to perform the mission;

- he technologies necessary to perform the mission; and
- he transitional processes for implementing new technologies in response to changing mission needs.

And includes :

- baseline architecture;
- target architecture; and
- sequencing plan.

Environment of operation: The physical surroundings in which an information system processes, stores, and transmits information.

Evaluate Phase: Capital planning phase that requires IT investments to be reviewed once they are operational to determine whether the investments meet expectations.

Executive agency: Has the meaning defined in Title 41, Public Contracts section 133.

Expected Outcome: Projected end result of the initiative (e.g., system(s) being replaced or improved customer service) that is directly linked with performance measures.

Feasibility Study: Preliminary research performed to determine the viability of the proposed initiative by performing an alternatives analysis including market research and extensive interviews with SMEs. Also includes a proposed technical approach and preliminary cost, scope, and schedule data.

Federal information: Information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

Federal information system: An information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency.

Federal Privacy Council: The Council established by Executive Order 13719.

Full Cost: All direct and indirect costs to any part of the Federal Government of providing goods, resources, and services (OMB Circular A–25: User Charges (July 8, 1993). The total amount of resources used to produce the output. More specifically, the full cost of an output produced by a responsibility segment is the sum of:

- he costs of resources consumed by the responsibility segment that directly or indirectly contribute to the output; and
- he costs of identifiable supporting services provided by other responsibility segments within the reporting entity and by other reporting entities.

Functional Requirements: A description of system capabilities or functions required to execute a required process such as a communication link between several locations and generating specific reports.

Funding: There are two types of funding for projects:

- ull funding means that appropriations are enacted that are sufficient in total to complete a useful segment of a capital project (investment) before any obligations may be incurred for that segment. When capital projects (investments) or useful segments are incrementally funded, without certainty if or when future funding will be available, it can result in poor planning, acquisition of assets not fully justified, higher acquisition costs, projects (investments) delays, cancellation of major projects (investments), the loss of sunk costs, or inadequate funding to maintain and operate the assets. Budget requests for full acquisition propose for full funding.

- ncremental (annual) funding means that appropriations are enacted that only fund an annual or other part of a useful segment of a capital project (investment). The OMB or the Congress may change the agency's request for full finding to incremental funding in order to accommodate more projects in a year than would be allowed with full funding.

Funding Source: Funding Source (or Fund Account Title, as defined in the OMB Circular A-11) refers to the direct appropriation or other budgetary resources an agency receives. Bureaus and offices need to identify the budget account and the budget authority provided. Report those budget accounts providing the financing for a particular IT investment. Where IT investment funding is provided in a manner such that "original paying accounts" within agencies are transferring resources to a different agency account which ultimately supports the IT investment (for example, when bureau accounts are paying into a central CIO office account or a WCF), the funding source provided in the Department IT Portfolio should be that of the account which ultimately pays contracts and other costs directly, for the IT investment, rather than the original paying accounts.

General Support Systems (GSS): Cross-Cutting Infrastructure Investment with a $5M annual cost or in excess of $35M lifecycle cost.

Government publication: Information that is published as an individual document at Government expense, or as required by law, in any medium or form.

Hardware or Equipment: Includes any equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information (e.g., computers and modems); capital and non-capital purchases or leases.

Hybrid control: A security or privacy control that is implemented for an information system in part as a common control and in part as a system-specific control.

Incident: An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Independent Verification and Validation: An independent review conducted by persons separate from the management and operation of the investment or system.

Inflation: The proportionate rate of change in the general price level as opposed to the proportionate increase in a specific price. Inflation is usually measured by a broad-based price index such as the implicit deflator for Gross Domestic Product or the Consumer Price Index.

Information: Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms.

Information dissemination product: Any recorded information, regardless of physical form or characteristics, disseminated by an agency, or contractor thereof, to the public.

Information life cycle: The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion.

Information resources: Information and related resources, such as personnel, equipment, funds, and information technology.

Information resource management: The process of managing information resources to accomplish agency missions. The term encompasses an agency's information and the related resources, such as personnel, equipment, funds, and information technology.

Information Resource Management Strategy: A strategy that demonstrates how information resources management decisions are integrated with organizational planning, budget, procurement, financial management, human resources management, and program decisions.

Information security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

- ntegrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;
- onfidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- vailability, which means ensuring timely and reliable access to and use of information.

Information security architecture: An embedded, integral part of the enterprise architecture that describes the structure and behavior of the enterprise security processes, information security systems, personnel, and organizational subunits, showing their alignment with the enterprise's mission and strategic plans.

Information security continuous monitoring: Maintaining ongoing awareness of information security, vulnerabilities, threats, and incidents to support agency risk management decisions.

Information security continuous monitoring program: The compendium of methods, tools, and techniques necessary to implement the agency information continuous monitoring strategy in a way that is sufficient to inform risk-based decisions and maintain operations within established risk tolerances. The program includes determining monitoring metrics, establishing monitoring frequencies, and developing a monitoring architecture.

Information security continuous monitoring strategy: A comprehensive plan to address monitoring requirements and activities at each organizational tier (organization, mission or business process, and information system).

Information system security plan: A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

Information security program plan: A formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.

Information system: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information system life cycle: All phases in the useful life of an information system, including planning, acquiring, operating, maintaining, and disposing.

Information system resilience: The ability of an information system to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities, and to recover to an effective operational posture in a time frame consistent with mission needs.

Information technology: Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such services or equipment if used by the agency directly or is used by a contractor under a contract with the agency that requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product. The term “information technology” includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources. The term “information technology” does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use.

Information technology investment: An expenditure of information technology resources to address mission delivery and management support. This 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. These investments shall 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 Investment Management: A decision-making process that, in support of agency missions and business needs, provides for analyzing, tracking, and evaluating the risks, including information security and privacy risks, and results of all major investments made by an agency for information systems. The process shall cover the life of each system and shall include explicit criteria for analyzing the projected and actual costs, benefits, and risks, including information security and privacy risks, associated with the investments.

Information technology resources: All agency budgetary resources, personnel, equipment, facilities, or services that are primarily used in the management, operation, acquisition, or other activity related to the life cycle of information technology; acquisitions or interagency agreements that include information technology and the services or equipment provided by such acquisitions or interagency agreements; but does not include grants that establish or support information technology not operated directly by the Federal Government.

Information Technology Systems for National Security: Section 5142 of ITMRA defines a national security system as follows:

- EFINITION - In this subtitle, the term "national security system" means any telecommunications or information system operated by the United States Government, the function, operation, or use of which:
  - nvolves intelligence activities;
  - nvolves cryptologic activities related to national security;
  - nvolves command and control of military forces;
  - nvolves equipment that is an integral part of a weapon or weapons system; or
  - ubject to subsection is critical to the direct fulfillment of military or intelligence missions.
  -

- IMITATION – Subsection:
    - Does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

Infrastructure: The IT operating environment (e.g., hardware, software, and communications).

Initial authorization: The initial risk determination and risk acceptance decision based on a zero-base review of the information system conducted prior to its entering the operations or maintenance phase of the system development life cycle. The zero-base review includes an assessment of all security and privacy controls (i.e., system-specific, hybrid, and common controls) contained in an information system security plan or in a privacy plan and implemented within an information system or the environment in which the system operates.

Interagency agreement: For the purposes of this document, a written agreement entered into between two or more Federal agencies that specifies the goods to be furnished or tasks to be accomplished by one agency (the servicing agency) in support of the other(s) (the requesting agency), including assisted acquisitions as described in the OMB Memorandum: Improving the Management and Use of Interagency Acquisitions and other cases described in FAR Part 17.

Integrated Project Teams (IPT): The OMB and the Department require that any bureau and office IT investment planning to perform any DME must establish an IPT. An IPT refers to a cross-functional or multidisciplinary group of individuals organized and collectively responsible for the specific purpose of delivering a project, product, or process to an external or internal customer. An IPT must include at a minimum: a qualified, fully dedicated IT program manager; a contracting specialist, if applicable; an IT specialist; an IT security specialist; and a business process owner or SME.

IT Portfolio: Combination of all IT assets, resources, and investments that an organization owns. The IT Portfolio considers new proposals along with previously funded investments to identify the appropriate mix and synergies of IT investments that best meet organizational, mission, and technological needs.

Lifecycle: The duration of the system life typically organized into four phases: initiation, development, operation, and disposal.

Lifecycle Benefits: The overall estimated benefits for a particular program alternative over the time period corresponding to the life of the program including:

- ost or expense reduction (productivity and headcount);
- ther expense reductions (operational);
- ost or expense avoidance; and
- evenue-related savings.

Lifecycle Cost: The overall estimated cost for a particular program alternative over the time period corresponding to the life of the program including direct and indirect initial costs plus any periodic or continuing costs of operation and maintenance.

Major Investment: Per the OMB, a major IT investment refers to an IT investment requiring special management attention because of its importance to the mission or function to the government; significant program or policy implications; high executive visibility; high development, operating, or maintenance costs; unusual funding mechanism; or defined as major by the agency's capital planning and IT investment control process. The OMB may work with the agency to declare IT investments as major IT investments. Agencies should consult with assigned OMB analysts regarding which IT investments are considered “major.” IT investments not considered “major” are considered “non-major.” The Department’s major IT investments include at least one of the following:

- IT investments previously reported to the OMB as major IT investments unless approved by the Department for non-major categorization or decommissioning;
- $5M annual cost or > $35M lifecycle cost;
- Importance to the mission or significant role in administration of programs, finances, property, or other resources;
- Integral part of the Department’s Enterprise Roadmap;
- Mandated by legislation or executive order, or identified by the Secretary as critical;
- Greater than $1M DME in the current FY;
- High risk as determined by the OMB, GAO, Congress and/or the CIO; and
- E-Government, Departmental, cross-cutting/Enterprise-wide (across more than one office or bureau).

Mission Analysis: Analysis of current and forecasted mission capabilities in relationship to projected demand for services.

Modular Development Approach: The OMB and the Department require that any bureau and office IT investment planning to perform any DME must leverage a modular development approach to focus on on-time delivery. Incremental development is required with deliverables not to exceed 90-120 day increments. More information and guidance can be found within the OMB’s Contracting Guidance for Modular Development.

Non-Developmental Item (NDI): Any previously developed item of supply used exclusively for governmental purposes by a Federal agency, a State, or local government that requires only minor modifications or modifications of a type customarily available in the commercial marketplace.

Non-Major Investments: Investments that are not considered “major” are classified as “non-major”.

Ongoing authorization: The risk determinations and risk acceptance decisions subsequent to the initial authorization, taken at agreed-upon and documented frequencies in accordance with the agency’s mission or business requirements and agency risk tolerance. Ongoing authorization is a time-driven or event-driven authorization process whereby the authorizing official is provided with the necessary and sufficient information regarding the security and privacy state of the information system to determine whether the mission or business risk of continued system operation is acceptable.

Operations and Maintenance (O&M) and Steady State (SS): Per OMB, O&M and SS are the maintenance and operation costs at the current capability and performance level including costs for personnel, maintenance of existing information systems, corrective software maintenance, voice and data communications maintenance, and replacement of broken IT equipment. For major IT investments, this amount should equal the amount reported for maintenance and the associated FTE costs reported in the Major IT Business Cases. Examples of O&M/SS include:

- Technical Refresh (swapping out old HW with newer HW to perform the same function but improve performance);
- Upgrading/adding bandwidth capacity;
- Patch Management;
- Release Management (installing new releases of the same SW vs. new/full versions);
- Cleanup of existing directories performance;
- Monitoring and Management of existing network;
- Replacing or moving an existing office circuit from one location to another;
- IT service and support to end users; and
- Replacing defective HW with a new unit that is fundamentally the same but without defect.

Technical refresh is considered to be Steady State; however, if there is a change to the scope or capacity, that work and associated costs should be categorized as DME.

Open data: Publicly available data that are made available consistent with relevant privacy, confidentiality, security, and other valid access, use, and dissemination restrictions, and are structured in a way that enables the data to be fully discoverable and usable by end users. Generally, open data are consistent with principles, explained in the OMB guidance, of such data being public, accessible, machine-readable, described, reusable, complete, timely, and managed post-release.

Outcome Measure: Outcomes describe the intended result of carrying out a program or activity. Outcome measure indicates progress against achieving the intended result of a program. Indicates changes in conditions that the Government is trying to influence.

Outlay: The issuance of checks, disbursement of cash, or electronic transfer of funds made to liquidate a federal obligation. Outlays also occur when interest on the Treasury debt held by the public accrues and when the Government issues bonds, notes, debentures, monetary credits, or other cash-equivalent instruments in order to liquidate obligations. Also, under credit reform, the credit subsidy cost is recorded as an outlay when a direct or guaranteed loan is disbursed.

Output Measure: A type of measure, specifically the tabulation, calculation, or recording of activity or effort usually expressed quantitatively. Outputs describe the level of activity that will be provided over a period of time. Outputs refer to the activities or products of a program. While output measures can be useful, there must be a reasonable connection between outputs used as performance indicators and outcomes. Agencies should select output measures based on evidence supporting the relationship between outputs and outcomes, or in the absence of available evidence, based on a clearly established argument for the logic of the relationship.

Overlay: A specification of security or privacy controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems.

Payback Period: The number of years it takes for the cumulative dollar value of the benefits to exceed the cumulative costs of an investment.

Personally identifiable information: Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Performance Indicator: What is to be measured including the metric to be used (e.g., conformance, efficiency, effectiveness, costs, reaction, or customer satisfaction), scale (e.g., dollars, hours, etc.), formula to be applied (e.g., percent of "a" compared to "b," mean time between failures), or conditions under which the measurement will be taken (e.g., taken after system is operational for more than 12 hours, adjusted for constant dollars, etc.).

Performance Measures: Method used to determine the success of an initiative by assessing the investment contribution to predetermined strategic goals. Measures are quantitative (e.g., staff-hours saved, dollars saved, reduction in errors, etc.) or qualitative (e.g., quality of life, customer satisfaction, etc.).

Portfolio: A set of programs, projects or other work grouped together to meet strategic goals and objectives.

Pre-Select Phase: Capital planning phase that provides a process to assess whether IT investments support strategic and mission needs.

Privacy continuous monitoring: Maintaining ongoing awareness of privacy risks and assessing privacy controls at a frequency sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.

Privacy continuous monitoring program: An agency-wide program that implements the agency's privacy continuous monitoring strategy and maintains ongoing awareness of threats and vulnerabilities that may pose privacy risks; monitors changes to information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and conducts privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at an agency across the agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks.

Privacy continuous monitoring strategy: A formal document that catalogs the available privacy controls implemented at an agency across the agency risk management tiers and ensures that the controls are effectively monitored on an ongoing basis by assigning an agency-defined assessment frequency to each control that is sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.

Privacy control: The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks.

Privacy control assessment: The assessment of privacy controls to determine whether the controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage privacy risks. A privacy control assessment is both an assessment and a formal document detailing the process and the outcome of the assessment.

Privacy impact assessment: An analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. A privacy impact assessment is both an analysis and a formal document detailing the process and the outcome of the analysis.

Privacy program plan: A formal document that provides an overview of an agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the Senior Agency Official for Privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.

Privacy plan: A formal document that details the privacy controls selected for an information system or environment of operation that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls.

Program management control: In the context of information security and privacy, a control that is generally implemented at the agency level, independent of any particular information system, and essential for managing information security or privacy programs.

Program Risk-Adjusted Budget (PRB): The total budget that represents the amount of resources and schedule expected to be needed to cover the risk of cost and schedule overruns to meet a 90 percent probability of project/program success. It is an amount held at a level above the program level to be released to the program when needed to cover risk that was not identifiable through an IBR, but that history indicates will cause cost and schedule overruns from the Performance Measurement Baseline through no fault of the program management process.

Project: A temporary endeavor to create a unique product or service with a start date, a completion date, and a defined scope.

Project Charter: A document issued by senior management that provides the PM with the authority to apply organizational resources to project activities.

Project Plan: A document that describes the technical and management approach to carrying out a defined scope of work including the project organization, resources, methods, and procedures and the project schedule.

Project Sponsor: Defines business needs and associated capabilities, risks, benefits, and costs of an investment.

Provisioned IT Service
An information technology service that is owned, operated, and provided by an outside vendor or external government organization, and consumed by the agency.

Public information: Any information, regardless of form or format, that an agency discloses, disseminates, or makes available to the public.

Reauthorization: The risk determination and risk acceptance decision that occurs after an initial authorization. In general, reauthorization actions may be time-driven or event-driven; however, under ongoing authorization, reauthorization is typically an event-driven action initiated by the authorizing official or directed by the Risk Executive (function) in response to an event that drives risk above the previously agreed-upon agency risk tolerance.

Records: All recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.

Records management: The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

Resilience: The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

Return: The difference between the value of the benefits and the costs of an investment. In a CBA, it is computed by subtracting the Total Discounted Costs from the Total Discounted Benefits; and it is called the Total NPV.

Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of:

- The adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and
- The likelihood of occurrence.

Risk management: The program and supporting processes to manage risk to agency operations (including mission, functions, image, and reputation), agency assets, individuals, other organizations, and the Nation, and includes:

- Establishing the context for risk-related activities;
- Assessing risk;
- Responding to risk once determined; and
- Monitoring risk over time.

Risk Management Plan: A description of potential cost, schedule, and performance risks and impact of the proposed system to the infrastructure. Includes a sensitivity analysis to articulate the effect different outcomes might have on diminishing or exacerbating risk. Provides an approach to managing all potential risks.

Risk management strategy: The description of how an agency intends to assess risk, respond to risk, and monitor risk, making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions.

Risk response: Accepting, avoiding, mitigating, sharing, or transferring risk to agency operations, agency assets, individuals, other organizations, or the Nation.

Security: Measures and controls that ensure the confidentiality, integrity, availability, and accountability of the information processes stored by a computer.

Security category: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on agency operations, agency assets, individuals, other organizations, and the Nation.

Security control: The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.

Security control assessment: The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.

Security control baseline: The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.

Security Plan: Description of system security considerations such as access, physical or architectural modifications, and adherence to Federal and the DOI security requirements.

Select Phase: Capital planning phase used to identify all new, ongoing, and operational investments for inclusion into the IT portfolio.

Senior Agency Official for Privacy: The senior official, designated by the head of each agency, who has agency-wide responsibility for privacy, including implementation of privacy protections; compliance with Federal laws, regulations, and policies relating to privacy; management of privacy risks at the agency; and a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals.

Senior Agency Official for Records Management: The senior official who has direct responsibility for ensuring that the agency efficiently and appropriately complies with all applicable records management statutes, regulations, NARA policy and OMB policy.

Sensitivity Analysis: An analysis of how sensitive outcomes are to changes in assumptions. Assumptions about the dominant cost or benefits elements and the areas of greatest uncertainty deserve the most attention.

Software: Any software, including firmware, specifically designed to make use of and extend the capabilities of hardware or equipment.

Steady State Phase: Capital planning phase that provides the means to assess mature IT investments to ensure they continue to support mission, cost, and technology requirements.

Strategic Goal: A statement of aim or purpose that is included in a strategic plan. Strategic goals articulate clear statements of what the agency wants to achieve to advance its mission, and address relevant national problems, needs, and challenges. Each performance goal should relate to the strategic goals of the agency.

Sunk Cost: A cost incurred in the past that cannot be recovered which may or may not affect present or future decisions.

Supply chain: A linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.

Supply chain risk: Risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Support Costs: Costs of activities not directly associated with production. Typical examples are the costs of automation support, communications, postage, process engineering, and purchasing.

System-specific control: A security or privacy control for an information system that is implemented at the system level and is not inherited by any other information system.

Systems security engineering: A specialty engineering discipline of systems engineering. It applies scientific, mathematical, engineering, and measurement concepts, principles, and methods to deliver, consistent with defined constraints and necessary trade-offs, a trustworthy asset protection capability that satisfies stakeholder requirements; is seamlessly integrated into the delivered system; and presents residual risk that is deemed acceptable and manageable to stakeholders.

Tailoring: The process by which security control baselines are modified by identifying and designating common controls; applying scoping considerations; selecting compensating controls; assigning specific values to agency-defined control parameters; supplementing baselines with additional controls or control enhancements; and providing additional specification information for control implementation. The tailoring process may also be applied to privacy controls.

Technical Requirements: Description of hardware, software, and communications requirements associated with the initiative.

TechStat: A face-to-face, evidence-based accountability review of an IT investment that enables the Federal Government to intervene to turn around, halt, or terminate IT projects that are failing or are not producing results for the American people.

Trustworthy information system: An information system that is believed to be capable of operating within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operation.

Appendix B - Acronyms

AA	Alternative Analysis
ACIO	Assistant Chief Information Officer
AD	Assistant Directors
AP	Acquisition Plan
BFIRM	Business Fiscal and Information Resources Management
BC	Business Case
BLM	Bureau of Land Management
BMC	Business Management Council
BO	Budget Office
BPR	Business Process Reengineering
bStat	BLM Status
BY	Budget Year
CAR	Corrective Action Report
CBA	Cost-Benefit Analysis
CCA	Clinger Cohen Act of 1996
CD	Center Director
CFO	Chief Financial Officer
CIO	Chief Information Officer
COTS	Commercial-Off-The-Shelf
CPIC	Capital Planning and Investment Control
CSBR	Cost, Schedule, Benefit, and Risk
CSAM	Cyber Security Assessment & Management
CV	Cost Variance
CV%	Cost Variance Percentage
CY	Current Year
DAC	Data Advisory Committee
DME	Development, Modernization and Enhancement
DOG	Deputies Operation Group
DOI	Department of the Interior
DSD	Deputy State Directors
EA	Enterprise Architecture
eCPIC	Electronic Capital Planning Investment Control
ELT	Executive Leadership Team
EOC	Explanation of Change
EVM	Earned Value Management
EVMS	Earned Value Management System
FAC-P/PM	Federal Acquisition Certification for Program and Project Managers
FAR	Federal Acquisition Regulation
FASA	Federal Acquisition Streamlining Act
FC	Field Committee
FDCCI	Federal Data Center Consolidation Initiative

FISMA	Federal Information Security Management Act
FITARA	Federal Information Technology Acquisition Reform Act
FY	Fiscal Year
GAO	Government Accountability Office
GPEA	Government Paperwork Elimination Act of 1998
GPRA	Government Performance and Results Act of 1993
GSC	Geospatial Steering Committee
HW	Hardware
IDC	Integrated Data Collection
IPT	Integrated Project Team
InvM	Division of Investment Management
IT	Information Technology
ITMRA	Information Technology Management Reform Act
JCS	Joint Certification Statement
MAR	More Accurate Reporting
MNS	Mission Needs Statement
NOC	National Operations Center
O&M	Operations and Maintenance
OA	Operational Analysis
OMB	Office of Management and Budget
PBCR	Performance Baseline Change Request
PIA	Privacy Impact Assessment
PIR	Post-Implementation Review
PM	Project Manager
POG	Principles Operating Group
PRA	Paperwork Reduction Act
RMP	Risk Management Plan
ROI	Return on Investment
RRC	Rating and Ranking Committee
SD	State Director
SFFAC	Statements of Federal Financial Accounting Concepts
SFFAS	Statements of Federal Financial Accounting Standards
SME	Subject Matter Expert
SS	Steady State
SV	Schedule Variance
SV%	Schedule Variance Percentage
SW	Software
WBS	Work Breakdown Structure
WCF	Working Capital Fund
WO	Washington Office

Appendix C - References

1. ***ITIB Charter***: Charter of the IT Investment Board, Bureau of Land Management, November 2013.
2. ***Field Committee Charter***: Charter of the Field Committee, Bureau of Land Management, May 2014.
3. ***Business Management Council Charter***: Charter of the Business Management Council, Bureau of Land Management.
4. ***Geospatial Steering Committee Charter***: Charter of the Geospatial Steering Committee, Bureau of Land Management, January 2016.
5. ***FAC-P/PM***: Revisions to the Federal Acquisition Certification for Program and Project Managers (FAC-P/PM), Office of Management and Budget, December 2013.
6. ***Contracting Guidance to Support Modular Development***: Office of Management and Budget, June 2012.
7. ***Handbook for Procuring Digital Services Using Agile Processes***: TechFAR, Office of Management and Budget, August 2014.
8. ***Assessing Risks and Returns***: A Guide for Evaluating Federal Agencies' IT Investment Decision-Making, U.S. General Accounting Office, Accounting and Information Management Division, February 1997.
9. ***Bureau of Land Management's IT Security Plan***, Bureau of Land Management, April 2002.
10. ***Circular A-11***: Preparation, Submission and Execution of the Budget, Office of Management and Budget, July 2016.
    a. ***Capital Programming Guide***, Office of Management and Budget, June 2006.
    b. ***Section 55 - Information Technology Investments***, Office of Management and Budget, 2016. https://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/s55.pdf
11. ***Circular A-76***: Performance of Commercial Activities, Office of Management and Budget, May 29th 2003.
12. ***Circular A-94***: Discount Rates for Cost-Effectiveness, Lease Purchase, and Related Analyses, Office of Management and Budget, January 2015.
13. ***Circular A-127***: Financial Management Systems, Office of Management and Budget, January 2009.
14. ***Circular A-130***: Management of Federal Information Resources, Office of Management and Budget, July 28, 2016.
15. ***Citizen-Centered Governance***: *Customer Value Through Accountability, Modernization, and Integration, Second Edition;* A Progress Report, DOI, October 9, 2002.
16. ***Clinger-Cohen Act of 1996*** (formerly the Information Technology Management Reform Act [ITMRA]).
17. DOI Information Technology Capital Planning and Investment Control Guide (BLM WO IM – 2005-172 dated June 23, 2005).
18. ***Earned Value Management Systems*** *(EVMS) Basic Concepts*, Project Management Institute, Project Management Institute (PMI) Home Page
19. ***Executive Guide: Leading Practices in Capital Decision-Making***, U.S. General Accounting Office, Accounting and Information Management Division, December 1998.
20. ***Earned Value, Project Management,*** Fleming, Quentin W., Joel M. Koppelman, Second Edition, Project Management Institute, Inc., 2000.

21. ***Federal Information Technology Acquisition Reform Act (FITARA),*** Title VIII, Subtitle D of the National Defense Authorization Act (NOAA) for Fiscal Year 2015, Pub. L. No. 11 3-29, December 2014.
22. ***NIST SP 800-65 Integrating IT Security into the Capital Planning and Investment Control Process,*** *January 2005*
23. ***Principles of Engineering Economy,*** Grant, Eugene L., W. Grant Ireson**,** Fifth Edition, The Ronald Press Company, 1970.
24. ***Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*** (Exposure Draft), U.S. Government Accountability Office, Accounting and Information Management Division, March 2004. http://www.gao.gov/new.items/d04394g.pdf
25. ***Smart Practices in Capital Planning***, The Federal CIO Council, Capital Planning and IT Management Committee, Industry Advisory Council (IAC), October 2000.

Appendix D – Capital Planning & Investment Control Website

For Policy Documents, User Guides, Capital Planning guidance, and templates please visit the Bureau of Land Management's Intranet site and select 'Information Resources Management' and follow the link to 'Capital Planning and Investment Control."