

Form 1221-2
(June 1969)



UNITED STATES
DEPARTMENT OF THE INTERIOR
BUREAU OF LAND MANAGEMENT

Release: 1-1718

Date: 08/27/2009

MANUAL TRANSMITTAL SHEET

Subject

1265 – Information Technology Investment Management (ITIM) [PUBLIC]

1. Explanation of Materials Transmitted: This release transmits Information Technology Investment Management (ITIM) policy, a new Manual Section, that describes the roles and responsibilities related to the ITIM processes.

2. Reports Required: None

3. Material Superseded: None

4. Filing Instructions: File as directed below

REMOVE

None

INSERT

Manual 1265
(Total 8 Sheets)

/s/ Ronnie Levine

Assistant Director
Information Resources Management

[This page is intentionally left blank]

Table of Contents

- .01 Purpose
- .02 Objectives
- .03 Authority
- .04 Responsibility
- .05 References
- .06 Policy
- .07 File and Records Maintenance
- .08 Process Overview

Glossary of Terms

Handbook

H-1265-1 Capital Planning and Investment Control

.01 Purpose

This Manual Section establishes policy, assigns responsibilities, and addresses standards and procedures for complying with the Bureau of Land Management's (BLM) Information Technology Investment Management (ITIM) and Capital Planning and Investment Control (CPIC) processes. ITIM is a structured and integrated approach for managing IT investments. ITIM ensures that all IT investments (or projects) align with the BLM's mission and support its business needs while minimizing risks and maximizing returns throughout the investment's life cycle. ITIM relies on systematic selection, control, and on-going evaluation processes to ensure that the investment's objectives are met efficiently and effectively. CPIC outlines a framework for managing the BLM IT investment portfolio. It enables BLM to address strategic needs, optimize the allocation of limited IT resources, and comply with applicable regulations and guidance.

.02 Objective

The objectives of this Manual Section are to describe executive decision making, staffing and coordination, and process documentation. This is necessary in order to ensure BLM's IT investments address supportability within its prescribed technical operating environment, mitigate risk, and present a cohesive, cost effective approach to meeting the missions and business goals of the organization.

.03 Authority

A. The Clinger-Cohen Act of 1996 (CCA), also known as the Information Technology Reform Act (ITMRA), provides that the government IT shop be operated exactly as an efficient and profitable business would be operated. Acquisition, planning, and management of technology must be treated as a "capital investment." The CCA emphasizes an integrated framework of technology aimed at efficiently performing the business of Federal Agencies. The CCA attempts to eliminate impulse purchases of hardware and software. Additionally, the CCA provides specific direction to Agencies in the review and approval of their IT investments.

B. The Chief Financial Officers (CFO) Act of 1990 is a comprehensive piece of legislation enacted by Congress to reform federal financial management. 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.

C. The Government Performance and Results Act (GPRA) of 1993 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.

D. The Federal Acquisition Streamlining Act (FASA) of 1994 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

E. The Paperwork Reduction Act (PRA) of 1995 significantly changes many aspects of information collection by the Federal Government. 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 the Office of Management and Budget (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.

F. The Government Paperwork Elimination Act (GPEA) of 1998 requires Federal Agencies to allow individuals or entities that deal with the Agencies the option to submit information or transact with the Agencies electronically, when practicable, and to maintain records electronically, when practical. The Act 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 encourages Federal Government use of a range of electronic signature alternatives.

G. The Federal Information Security Management Act (FISMA) requires that each Federal agency shall develop, document, and implement a single information security program to provide information security for the information and information systems that support the operations and assets of the agency.

H. The E-Gov Act of 2002 requires all Executive Branch Agencies conduct a Privacy Impact Assessment (PIA) 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.

This document implements specific information technology (IT) requirements of these laws. The BLM ITIM process is authorized and maintained by the Chief Information Officer (CIO) and is consistent with the Office of Management and Budget (OMB), Government Accountability Office (GAO), and Department of the Interior (DOI) guidance.

.04 Responsibility

A. The Assistant Director, IRM is responsible for approving all IT expenditures to ensure that adequate resources are available to support the functions required by OMB Circular A-130 and the DOI and to ensure that those expenditures are in accord with the BLM's enterprise architecture and capital planning policies and procedures. AD-IRM is the BLM's designated Chief Information Officer (CIO). The CIO oversees BLM compliance with Federal and Departmental policies, guidelines, and regulations governing the management of IT investments and assets. The CIO develops and institutes a structured IT CPIC process for BLM.

B. Assistant Directors (AD's) are officially designated as the owners of information systems and data supporting the program areas within their jurisdictions. AD's are responsible for ensuring that CPIC process objectives are carried out within their areas of responsibility and that skilled IRM advisors and project managers are assigned to oversee and manage all IT investments under their span of control.

C. State Directors (SD's) and Center Directors (CD's) are responsible for ensuring that the CPIC process objectives are carried out within their organizations for those IT assets and investments within their areas of responsibility. Additionally, they ensure that qualified project managers are assigned for all formal IT activities designated as projects. SD's and CD's are the system owners for IT assets and information unique to their organizations.

D. Organizations responsible for ensuring that proposed investments meet the BLM's strategic, business, and technical objectives are:

1. Information Technology Investment Board (ITIB) – Roles and responsibilities are outlined in the ITIB Charter that can be found at the BLM CPIC Website. The ITIB is responsible for selecting, controlling, and evaluating all IT enterprise and national level IT investments. The ITIB is the governing board which reviews executive input and recommendations in order to make effective decisions on IT investments across the BLM. Additionally, the ITIB serves as a forum for executive level evaluation and control of the use and cost of BLM information systems (software) and technology (hardware and infrastructure) investments.
2. BLM State, Center, and Washington Offices (WO) – States, Centers, and the WO are responsible for selecting, controlling, and evaluating all IT investments unique to those Offices which do not exceed \$500K in total life-cycle costs. States, Centers, and the WO 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.

E. Offices and Personnel - The following support staff, offices, officially sanctioned national teams, and/or functionally designated personnel are responsible for implementing and executing the ITIM and CPIC processes:

1. System Owner – A system owner may be an AD, SD, or CD having assigned responsibilities to ensure that all IT assets and information which comprise an automated system are evaluated on an annual basis and receive an appropriate level of funding for operations and maintenance. The system owner is also responsible for identifying and assigning project sponsors, project managers, system managers and/or user representatives.
2. Project Sponsor – A project sponsor may be a WO, State, Center, or Field Office manager who authorizes the development of a business case. The project sponsor is responsible for providing programmatic oversight and support to a project manager throughout the life cycle of the investment which includes approving all budget

planning, funding, accounting, adjusting, and auditing activities in order to ensure fiscal integrity through the implementation and exercise of adequate financial controls. The project sponsor's role diminishes and may be terminated or re-assigned to the system manager/user representative by the system owner when the project reaches operational status.

3. Project Manager – The project manager is responsible for development of all proposals, plans, budgets, documentation, contractual and organizational/staffing requirements, and briefing materials associated with a formally designated IRM project. The project manager reports directly to the project sponsor and reports on all applicable matters to the ITIB. Ultimately, the project manager is responsible for the successful management and completion of one or more projects approved by the ITIB.
4. System Manager/User Representative – User representatives provide program oversight of operationally deployed systems. Generally, the system manager and the user representative are the same official unless the scope, size, or complexity of the system warrants multiple user representatives. The user representative is the focal point of contact for mission/program personnel who use the application system in carrying out their work and that of BLM. User representatives collect information on system performance, errors, improvement requests, training needs, and policy changes which affect system operational requirements. The user representative follows established procedures for communicating these matters to the project manager or designated IRM personnel who maintain the application or who conduct development work.
5. Division of Investment Management (AD-550) – This Division, within the AD-IRM Directorate, is responsible for monitoring all IT investments and projects to ensure they are aligned with the ITIM's Select, Control and Evaluate criteria. AD-550 coordinates with other organizations to ensure that projects are consistent with the BLM's Architecture, Security, Records, and functional policies and requirements. Additionally, as the conduit to the ITIB, this organization monitors the project's performance (scope, schedule, and budget) during the Control Phase of the project's life cycle and coordinates all other national IT investments and acquisition management activities falling under the purview of IRM CPIC. This team is also responsible for developing and modifying the IT Portfolio selection criteria for ITIB approval.
6. Chief Information Officers Council (CIOC): The CIOC consists of State and Center CIOs responsible for their jurisdictional IRM operations and the IRM Advisors responsible for the coordination of national business applications. Operating under the authority of the BLM CIO, the Chairman of the CIOC advises the BLM's CIO, the National Operations Center, and senior management on information resources management and information technology issues.

.05 References

MS-1220 Records and Information Management
MS-1264 Information Technology Security
MS-1268 Information Technology Configuration Management

.06 Policy

It is the policy of BLM that all IT investments are monitored, tracked, documented, maintained, validated, controlled, and released under the BLM ITIM and CPIC processes. The corresponding BLM Handbook, H-1265-1, Capital Planning and Investment Control, documents the processes and activities necessary to ensure BLM's IT investments address supportability within prescribed technical operating environments, mitigate risk and present a cohesive, cost effective approach to meeting OMB, GAO, and DOI objectives.

The scope of the policy contained in this document applies to all BLM resources at all levels. This policy is mandatory for all organizational units, employees, contractors, and others having access to and/or using the IRM resources of the BLM. This Manual will be applied to all existing and future IT investments. It will also be applied to all internal Service Level Agreements (SLAs) between organizational units and external interagency agreements and contracts made between BLM and other public and private organizations.

.07 File and Records Maintenance

Maintain and dispose of all files in accordance with BLM/General Records Schedule (GRS), 27, item 3.

.08 Process Overview

At the highest level, the ITIM and CPIC processes can be represented as a circular flow of BLM's IT investments through four sequential phases. The key goal is to align mission and program technical requirements with budget formulation and execution for all significant IT investments. These phases are shown in Figure 1 below:

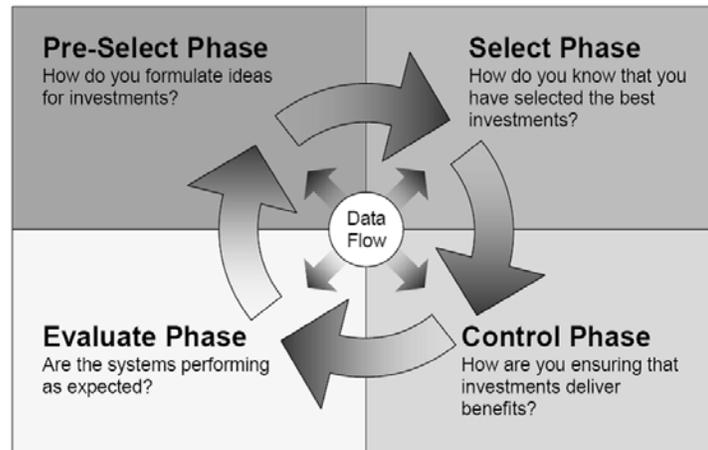


Figure 1: CPIC Phases

A. **Pre-Select Phase:** This is an initial screening process. When IT investments are proposed, executive decision makers assess each proposed investment's support of BLM's strategic and mission needs and potential for business improvement.

B. **Select Phase:** During this phase, IT project comparison, evaluation, and prioritization occurs. IT project investment analyses are conducted to assist the ITIB in selecting and prioritizing IT investments that best support the BLM missions in alignment with fiscal year budget dynamics.

C. **Control Phase:** This phase consists of governance, oversight, and follow up to insure cost effective management occurs. Through timely oversight, quality control, and executive review, BLM ensures that IT initiatives are executed and developed according to pre-approved schedule and milestones in a disciplined, well-managed, and consistent manner.

D. **Evaluate Phase:** During evaluation, investments are assessed to determine how well they are meeting planned objectives. Actual results of the implemented projects are compared to expectations to assess the investment's performance. This is done to measure and document the investment's impact on mission performance, identify any investment changes or modifications that may be needed, and revise the investment management process based upon lessons learned.

Glossary of Terms

BLM Enterprise Architecture (BEA) – At its core, the BEA is about the work that the BLM does and the information that it uses to accomplish the work. It is a management framework that describes “what” needs to happen rather than “how” it should happen; the business rules and processes (including information and data) required to operate the organization that are independent of any specific organizational structure, technology, or existing systems; and the hardware and software needed in basic operations of the BLM.

Capital Planning and Investment Control (CPIC) – A systematic approach to selecting, managing, and evaluating information technology investments. CPIC is mandated by the Clinger Cohen Act of 1996 which requires Federal Agencies to focus more on the results achieved through IT investments while streamlining the federal IT procurement process.

Information Technology (IT) – The hardware and software that processes information to accomplish a function, regardless of the technology involved, whether computers, telecommunications, or others. It includes automatic data processing equipment as that term is defined in Section 111(a) (2) of the Federal Property and Administrative Services Act of 1949.

IT Investment – A managerial decision to expend resources to obtain IT or IT-related assets that produce organizational benefits (such as reducing costs, creating new benefits, reducing cycle time, etc.).

IT Investment Management – An integrated process that provides for continuous identification, selection, control, life-cycle management, and evaluation of IT investments.

IT Project – A managed organizational initiative that develops or produces IT or IT-related assets that should result in the expected organizational benefits.

Lifecycle – The entire useful life of a product or service, usually divided into phases including initiation, development, execution, operation and maintenance, and disposal or termination.

Project Lifecycle – Collection of general sequential phases that include the steps necessary to conceptualize, design, develop and deploy (but not operate or dispose of) the project’s performance deliverables.

Project Management – The application of knowledge, skills, tools, and techniques to plan and execute tasks that meet or exceed customer/stakeholder needs and expectations from a project.

Risk – A discrete, possible future occurrence that may affect a project for better or worse.

Risk Management – An integral part of project management that includes the processes required to identify, quantify, respond to, and control project risk.

Service-Level Agreement (SLA) – A negotiated agreement between two parties where one is the customer and the other is the service provider. The SLA records a common understanding about services, priorities, responsibilities, guarantees and warranties.