Form 1221-2
(June 1969)

UNITED STATES
DEPARTMENT OF THE INTERIOR
BUREAU OF LAND MANAGEMENT

MANUAL TRANSMITTAL SHEET

Release
1-1680
Date
04/03/03

Subject H-1268-1 **Bureau of Land Management Configuration Management Handbook**

1. Explanation of Material Transmitted: This release transmits Configuration Management (CM) policy, a new Handbook Section that provides direction for conducting configuration management activities for the Bureau of Land Management's Information Technology (IT) hardware, software, and Commercial-off-the-shelf (COTS) products. CM is the process the BLM uses to manage, track, and document changes, to validate and test requirements, to ensure information is clear, concise, and valid, and to distribute and communicate changes to an IT asset throughout its life cycle.

2. Reports Required: None.

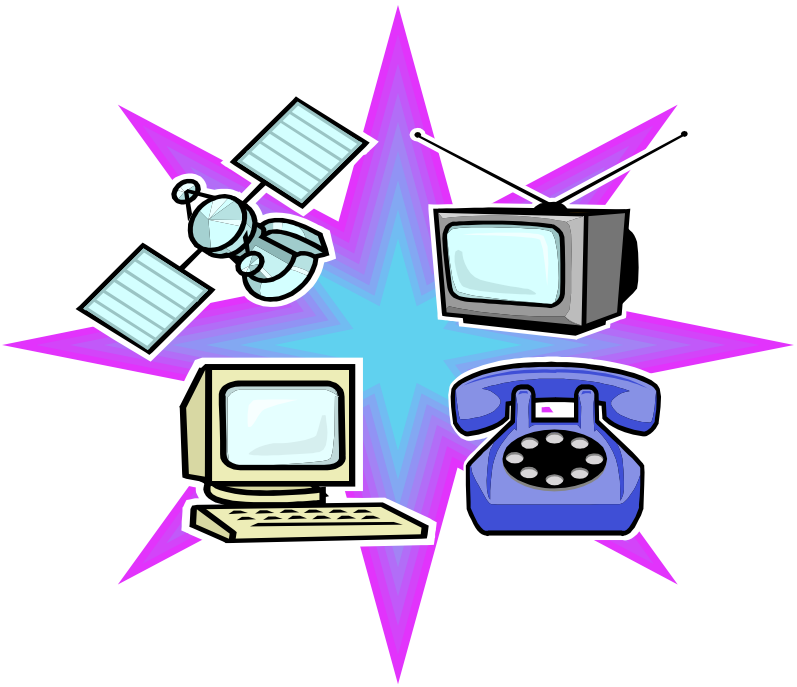
3. Material Superceded: None.

4. Filing Instructions: File as directed below.

REMOVE :	INSERT :
None	H-1268-1
	(Total: 56 Sheets)

Michael J. Howell Jr

Assistant Director
Information Resources Management



Bureau of Land Management

Configuration Management Handbook

TABLE OF CONTENTS

Chapter 1 Introduction

1.0 Introduction

Configuration Management (CM) is a disciplined approach to managing Information Technology (IT) assets based on industry standards and models. It is one of the key processes the Bureau of Land Management (BLM) uses to formally manage its IT assets throughout their life cycle.

Chapter 1 provides an overview of the CM process and its goals and objectives. It addresses the National, State, National Center, and Project level baselines describing their makeup and their relationship to the Technical Reference Model (TRM). It also provides guidance on how and when to use this handbook.

Chapter 2 describes the configuration management process, responsibilities, general rules, organizational relationships, the change management process, reporting requirements, approved communications, and delivery mechanisms.

Chapter 3 describes the documentation needed for configuration management such as forms, logs, plans, system design documents, and decision documents.

Chapter 4 describes the relationship with other Bureau core IT related activities. It also briefly describes the investment management process

Glossary

Appendices

1.1 An Overview of the CM Process

The BLM's CM process is based on the Institute of Electrical and Electronic Engineers (IEEE) standard and Systems Engineering Institute's (SEI) Capability Maturity Model (CMM) for software development and Institute of Configuration Management's CM II standards for process development. It is also based on life cycle management practices and is tailored to the BLM's Investment Management Process (IMP). It is designed to achieve consistent conformance and accommodate changes to the BLM's IT assets.

The BLM's CM process stresses uniformity and integration of activities to assure coordination and communication occur between the Bureau Program Offices, Executive Leadership, IT Security, Data, Records, and Architecture personnel. It also focuses on assuring that IT assets are tested, documented, monitored, and tracked throughout their life cycle.

The BLM's CM process activities are divided into three core areas:

Acquisition Configuration Management's (ACM) objective is to ensure that contracts for applications, systems, computer hardware, and telecommunications devices include language that clearly states deliverables in the form of system specifications and associated documents, a functionality matrix, system pilots, testing requirements, and associated user documentation. It is performed by acquirers regardless of the purchasing mechanism selected.

Hardware Configuration Management's (HCM) objective is to manage and maintain the integrity of BLM's desktops, servers, routers, radios, and other hardware with their correlating operating systems, installed software, firmware and/or accessories. HCM is typically performed by System Administrators, Network Administrators, Help Desk Technicians, and other computer support professionals.

Software Configuration Management's (SCM) objective is to manage changes, document, validate, and maintain the integrity of software assets throughout their life cycle. It covers in-house and external software development and commercial-off-the shelf (COTS) products. While SCM traditionally focused on software development activities, BLM expanded its role to include COTS and middleware. It is typically performed by systems engineers, and software and application developers.

Although the three core areas are linked, segregating CM process activities assist managers and employees with understanding that the responsibility for managing IT

assets is everyone's business. Additionally, it highlights the importance of managing changes to IT assets so that information about those assets is clear, concise, accurate, and valid to assist managers with making decisions, and reporting information to clients.

1.2 BLM CM Process Goals and Objectives

CM process goals support the following FY 2002 through FY 2005 Information Resources Management (IRM) Strategic Plan goals: (1) Improve Management of Information Technology Assets, (2) Enhance the Transformation of Data Into Knowledge, and (3) Support the Bureau's Mission by increasing the Effectiveness and Timeliness of Service Delivery and Effectiveness of its Human Capital. CM Process goals will be assessed at the beginning of each fiscal year for compliance to the IRM Strategic Plan. Table 1 outlines CM process goals and objectives.

Table 1 CM Process Goals And Objectives

Goal 1: The BLM will develop and maintain an integrated CM process to support its mission and the IRM Strategic plan.	
Objective 1	Integrate CM core process requirements with System Coordination Office (SCO), National Information Resources Management Center (NIRMC), States, National Centers, Field Offices (FO), and Assistant Directors (AD) to assure information integrity and accessibility.
Objective 2	Coordination and communication with all BLM employees to ensure changes to IT assets are managed to help managers make business decisions based on accurate and valid information.
Objective 3	Review products to ensure they are in compliance with existing IT architecture, data, records, and IT security.
Objective 4	Maintain historical records of BLM IT assets to ensure traceability.
Goal 2: The BLM will increase the application of CM principles within its program areas.	
Objective 1	Provide a process that ensures Quality Assurance, IT Security, Records, Architecture, and Data Management activities are followed.
Objective 2	Ensure Version Control is performed for existing and new systems.
Objective 3	Ensure BLM CM baselines are enforced.
Goal 3: The BLM will assure that its workforce understands CM.	
Objective 1	Disseminate CM product life cycle policies and procedures throughout the BLM.
Objective 2	Educate all employees about CM

1.3 Relationship Between IRM Strategic Goals and CM Process Goals

Table 2 illustrates the relationship between BLM's FY 2002 - FY 2005 IRM Strategic goals and the CM Process goals. An "N" indicates that the CM process goal is necessary to achieve the IRM Strategic goal. An "F" indicates that the CM process goal facilitates the achievement of the IRM Strategic goal.

Table 2 Relationship Between IRM Strategic Goals and CM Process Goals

BLM IRM Strategic Goals / **BLM CM Process Goals**	Improve Management of IT Assets	Enhance the transformation of Data Into Knowledge	Support the Bureau's Mission by increasing the effectiveness and Timeliness of Service Delivery and Effectiveness of its Human Capital
Develop and maintain an Integrated CM process	N	N	N
Increase the application of CM principles within its program areas.	N	N	N
Assure workforce understands CM.	F	F	N

1.4 Performance Measures

The Government Performance and Results Act of 1993 requires agencies to submit annual performance plans and prepare annual performance reports at the end of each fiscal year. Configuration Managers must develop performance measures to rate the effectiveness of the CM process.

Configuration Managers should consult with the National CM (NCM) staff on developing CM performance measures. Examples of CM performance measures are denoted in Table 3.

Table 3 CM Performance Measures		
Performance Measures	Performance Outcome	Product
Average percentage of time of Intranet Availability	Access to BLM IT asset information at anytime from any place	Web-based Up-to-date baseline and an Automated CM Library Repository
Reduce number of systems in noncompliance with the CM Process	Improved Accountability of BLM Systems (identification, testing, and implementation)	CM Manual and Handbook National, State, and National Center CM Operating Standards
Percentage of IT assets successfully deployed through the CM Process	Improved Communications	Training Materials, Briefings, Status Reports
Percentage of surveyed users satisfied with CM	Increased Customer Satisfaction	Customer Satisfaction Survey

1.5 Handbook Objectives

The CM Handbook and Manual form the foundation for the BLM's CM process. Table 4 outlines the Handbook's objectives.

Table 4 CM Handbook Objectives	
Objective 1	Implement policy described in the CM Manual.
Objective 2	Clarify organizational roles and responsibilities and their relationship to other processes in establishing a clear chain of custody to managing the BLM's IT assets.
Objective 3	Provide operational instructions to assist BLM employees with carrying out their day-to-day CM activities.
Objective 4	Provide samples of templates, forms, and plans needed for the CM process.

1.6 How To Use The Handbook

This Handbook describes how the policy outlined within the CM Manual will be implemented. Furthermore, the procedures documented serve as a resource for implementing a change management process for carrying out the BLM's CM activities throughout all levels of the organization. Employees must consult the Handbook or their local Configuration Manager when an IT asset is being planned, acquired, and when it arrives on site for compliance with the CM process.

Assistant Directors, State Directors, Chief Information Officers (CIO), and other senior level management officials may increase the level of management controls within the process, but may not decrease them. If management decides to supplement policy direction, the additional policy guidance must be clearly displayed and communicated throughout their jurisdiction and NCM.

1.7 The CM Baselines

The CM baselines represent a snapshot of all BLM approved IT assets at a particular moment in time. They are dynamic and are subject to change with each investment decision that leads to acquisition and deployment of an IT asset. According to the BLM's Investment Management Process investment decisions are made by IT Investment Boards, CIOs, Sponsors and other designated managerial officials. CM is the process used to document, test, validate, monitor, track, and communicate the outcome of those decisions prior to acceptance, deployment, and release to BLM.

CM baselines are tools used to maintain a record of those approved IT assets. They may serve as instruments for decision-makers to forecast usage of IT assets, examine emerging technological needs and offer an opportunity to consolidate maintenance renewals, acquire additional licenses or upgrade hardware to maximize savings. CM Baselines are maintained at the National, State, National Center and Project level. State, National Center, and Project level CM baselines should be similar to NCM baselines. The BLM's National Baselines will be categorized in four areas: As-Planned As-Released COTS and Applications, As-Planned As-Released Hardware, Software Product, and Hardware Product.

1.7.1 As-Planned As-Released Baseline

The As-Planned, As-Released COTS and Applications Baseline provides an overview of approved existing and future applications. It lists proposed configurations and final configurations. It may be used to help management officials plan workloads based on projected release schedules. It may also be

used to assist managers with planning for future hardware upgrades based on software releases and their correlating system requirements.

1.7.2 As- Planned As-Released Hardware Baseline

The As-Planned, As-Released Hardware Baseline provides an overview of approved future and existing hardware products. It lists proposed configurations and final configurations. It may be used to help management officials with refreshment planning. It may also be used to help management officials standardize on equipment to help reduce the price of support inherent with having multiple systems by multiple vendors.

1.7.3 Software Product Baseline

The Software Product Baseline provides a listing of all approved software by product name, vendor, release date, version number, contract number, system owner and sponsor. It also contains the number of licenses available in the Bureau. It may be used by management to make purchasing decisions.

1.7.4 Hardware Product Baseline

The Hardware Product Baseline provides a listing of all approved hardware by product name, vendor, release date, platform, and contract number. It may be used by management to make purchasing decisions.

1.8 The Technical Reference Model

The TRM provides a framework for future and existing architectural direction for the Bureau. It enables management to plan its upgrades or systems based on BLM's architectural direction. It is designed to assist managers in making sound IT purchasing decisions. The TRM's current category is aligned to CM's As-Released COTS, Applications and Hardware Product baselines. Because baselines tend to change rapidly, the TRM current category will display the products by vendor, release date, version number and will refer to the Hardware and Software baselines on the NCM web page.

1.9 The Investment Management Process

CM is an integral part of the Investment Management Process (IMP). Using the IMP establishes a clear chain of custody for decision-making for both National, State, and National Center IT assets. It also assigns accountability for authorizing changes to IT assets to the business owner. The BLM's IMP has three phases: Select, Control, and Evaluate. In the Select Phase, State and National Center Configuration Managers are responsible for assuring that sponsors assign system owners to each IT asset for decision-making and they assure that those decisions are tracked and their CM baselines are managed. At the National Level the responsibility is split between the System Coordination Office (SCO) staff and the Investment Management Group National Configuration staff: the SCO is responsible for assuring that sponsors assign a system owner, a project manager, and a user representative for each newly acquired IT asset; and the National Configuration Manager is responsible for assuring that the decisions are tracked and the NCM baseline information remains accurate throughout an IT asset's life cycle. Within the CM process, managing CM baseline information for accuracy and keeping it up-to-date is a function of Configuration Managers. It allows project proponents to bridge the gap between the IT Clearinghouse and its replacement system, and approved IT assets before pursuing new investment.

In the Control Phase, the Project Manager is responsible for using the CM process to ensure that system and user requirements are validated, documented, and testable. Project Configuration Boards are responsible for ensuring that documentation accurately reflects the IT asset. National, State, and National Center Configuration Managers are responsible for assuring that IT assets interoperate and integrate within BLM's existing environment. Additionally, they are responsible for assuring that all media and documentation (test plans, test cases, test descriptions, implementation schedules, system guides, user manuals, and associated documents) accurately reflect the IT asset scheduled for release.

In the Evaluate Phase, National, State, and National Center Configuration Managers are responsible for overseeing and coordinating version management for released IT assets to assure that information is available for system owners and sponsors to make decisions about bug fixes, patches, upgrades, and system improvements. The CM process provides the tools for tracking, monitoring, and communicating status on released IT assets.

1.10 Continuity of Operations Planning

All software and hardware configurations, documentation, and media associated with approved released software and hardware IT assets must be maintained and stored in a

secured facility with access documented in logs demonstrating a clear chain of custody. Personnel responsible for software and hardware configurations, media, and documentation must be listed in the site(s) Continuity of Operations Plan. Documentation, media, software, and hardware configurations should be restored and tested according to the Bureau's IT Security and Records Management policies.

Chapter 2 – The CM Process

2.0 The BLM CM Process

This chapter describes general principles, responsibilities, and the organizational structure of the CM process. Additionally, it describes the basic CM Process components, the Change Management Process (CMP) and the Baseline Management Process (BMP) in the three core areas: Acquisition Configuration Management (ACM), Hardware Configuration Management (HCM), and Software Configuration Management (SCM) with their associated activities. This process bridges the gaps between the Investment Management Process (IMP) and the Technical Reference Model (TRM) regarding managing information about IT assets and reporting that information through CM baselines. It uses the Institute of Electrical Electronic Engineers (IEEE) process standards for documentation and software development activities. Projects are expected to comply with the IEEE standard. To ensure BLM has access to the IEEE process standards information, BLM has invested in an enterprise license.

2.1 General Principles

The BLM CM process is built on the following foundation: (1) communicating and documenting how decisions are made; (2) managing changes to IT assets which include the application, software, hardware, system documentation, user guides, media, configurations, and associated tasks through tracking and monitoring IT assets through a clear chain of custody throughout their life cycle; (3) reporting changes to IT assets through baselines and status reports; (4) testing, documenting, and validating that IT assets perform as expected; (5) releasing and verifying that IT assets performed as expected; and (6) communicating the progress on delivery and use of IT assets.

2.1.1 Authorized Communication Methods

2.1.1.1 Web

CM web sites serve as one of the key communications mechanisms for information dissemination. Information is managed according to the CMP. That means that information is verified and validated before posting, and that the CMP is also posted and maintained on the web site. Status reports, meeting minutes, baseline information, a calendar of events, hot topics, agendas, CM documentation standards, forms, templates, checklists, charters, and all related CM documents are available from the site. The web site is the official source for the latest releases of CM information.

Configuration Managers will post large documents for review in portable document format (pdf) on the web site. What constitutes a large document will be described in Standard Operating Procedures (SOPs) for electronic records.

2.1.1.2 Electronic Mail

Electronic mail may be used by sponsors, system owners, project managers, and configuration managers to record decisions and communicate status. Those electronic records shall be retained according to Records Management policy. Configuration Managers may also use electronic mail to provide status on CM activities.

2.1.1.3 Directives

Configuration Managers will use the formal directives process to communicate policy and information on CM initiatives. Configuration Managers working with their CIOs should decide the appropriate communications mechanism for the situation.

Formal Directives Are Best Used For:

1. Communicating interim change to existing CM policy.

2. Distributing information about chartered groups and teams.

3. Communicating the release of IT assets to the CM baselines

4. Establishing the implementation by date of released IT assets

2.1.1.4 Meetings

Teleconferences and face-to-face meetings are necessary to coordinate activities and tasks. Meeting minutes serve to document records of decisions. Configuration Managers ensure that coordination occurs and that agendas are prepared for participants.

2.1.2 Authorized Delivery Mechanisms

Software and hardware IT assets may use several available delivery mechanisms

available to BLM. All released software is delivered to the Configuration Managers. There are two preferred methods of delivery for national software assets:

1. An enterprise management system for the distribution of software.

2. File transfer access through an electronic software repository maintained by the NIRMC Webmaster. The repository is password protected.

3. Traditional delivery systems like U.S. Mail, United Parcel Service, and Federal Express may also be used. States and National Centers may use the preferred methods of delivery through NIRMC.

2.2 Responsibilities

Everyone in BLM is responsible for CM. Therefore, it is critical that all employees and contract staff understand their role within CM process for maintaining and delivering sound IT solutions to assist programs in meeting their business objectives.

2.2.1 How Are BLM Employees Affected by the CM Process?

Past implementations of CM within BLM described the function and the discipline. Employees learned that CM should be applied to large-scale application development projects and it was applied using Military Standard (MilStd) 975 and 2167A.

With the application of the Clinger-Cohen Act within the BLM, the CM process takes on a coordination and integration role with existing established programs like Data Management, IT Security, and Records Management. It also is integrated into the IT IMP and the BLM's architectural effort. The CM process establishes the methodology for documenting, testing, reporting, and managing changes to IT assets. Every BLM employee is affected by the CM process. CM is not the process for making IT investment decisions, it complements the IMP and the Records Management Process for reporting those decisions.

2.2.2 User Responsibility

Each user is responsible for submitting problem reports to the BLM Help Desk and those users who author documents are responsible for using the CM process for managing changes to those documents as described in Section 2.5. Furthermore, each user is responsible for applying the IMP and CM processes to acquire, install and configure hardware and software IT assets.

For National, State, and National Center level systems, sponsors will assign user representatives to software IT assets. User representatives are responsible for serving on integrated project teams to review, test, and validate software/application functionality.

2.2.3 Help Desk Personnel Responsibility

Help Desk personnel are responsible for assigning ticket numbers, documenting and tracking problems throughout their resolution. They are responsible for reporting problems requiring the generation of a Change Request (CR) to their local Configuration Manager. Help Desk personnel may be assigned to product reviews, integrated or cross-functional project teams, and process improvement teams.

2.2.4 System Administrators Responsibility

System Administrators are responsible for managing the hardware and software desktop and server configurations. They are responsible for tracking changes and ensuring that systems are configured and maintained as documented. They serve as subject matter experts during software and hardware testing and for providing input to decisions on acquiring software and hardware.

2.2.5 Network Administrators Responsibility

Network Administrators are responsible for managing routers, hubs, gateways, and other local area network (LAN) and wide area network (WAN) devices. They are responsible for tracking changes and ensuring that network hardware and software systems are configured and maintained as documented. They serve as subject matter experts and may be called upon to conduct network performance monitoring and work on assessments, serve on cross-functional or integrated project teams.

2.2.6 Electronic Mail Administrators Responsibility

Electronic Mail Administrators are responsible for managing electronic mail servers and information ensuring that servers are configured and maintained as documented. They serve as subject matter experts on hardware and software needed to ensure electronic mail systems function as documented and needed**.** They may also serve on cross-functional or integrated project teams.

2.2.7 Configuration Managers Responsibility

Configuration Managers are responsible for overseeing the local CM Process and ensuring that employees understand the CM process. They are also responsible for assuring that newly acquired and existing IT assets are properly documented, controlled and distributed, and that baselines are accurate and maintained. They work with NCM and BLM's CIOs to shape CM policy and procedures. They provide advisory services to managerial officials and other BLM users. Furthermore, they are responsible for coordinating CM activities with their local IT Security Administrator, Records Administrator, Data Administrator, Help Desk personnel, project managers, system owners, and sponsors.

2.2.8 Management Officials

Managers are responsible for ensuring that their staffs comply with CM policy and that all employees understand it and know where to go for assistance. Management Officials are the only personnel within the Bureau responsible for directing employees to acquire an IT asset.

2.2.9 Cross-functional or Integrated Project Teams

Teams are responsible for verifying and validating that IT assets perform as stated. They may be used to assist with developing test plans, performing testing, conducting reviews, project implementation planning, and deployment. Teams may be directed by Project Managers, Configuration Boards, Technical Review Boards (TRBs), and other BLM managerial officials.

2.3 Reporting Requirements

2.3.1 CM Process Assessments

The National Configuration Manager will schedule assessments of the BLM CM process annually. Assessments serve to define current practices and capabilities relative to preferred practices and capabilities. The BLM CM process' success is directly proportional to BLM personnel's understanding the relationship between current practices and the preferred practices. The assessments will be used as a tool to educate senior level management, and to measure improvements in the CM process. Their results will be submitted directly to the CIO, and the final reports will be posted on the NCM website in pdf.

Additional assessments may be generated at the request of project managers, system owners, end-users, and managerial officials. The BLM CM process assessments may be conducted by internal or external resources. Assessments

will focus on the following three phases: core CM process requirements, enabling system requirements, and interfaces to other core processes. Table 5 provides examples of requirements within the three phases.

Table 5 Assessment Phases and Requirements

Phase	Category	Description	Requirement Example
Core CM Process Requirements	1.0	Administrative Hierarchy, Business Enterprise	CM SOP (Procedures are in place and accessible to employees.)
	2.0	Physical Item Hierarchies	Information Repositories and Security (Repositories are used to retain and secure the various types of IT assets and process-related information which could impact safety, quality, schedule, or cost.)
	3.0	Naming, Numbering	Standardized numbering conventions (Standardized numbering conventions are used to identify items and documents. Use of logs to control ID numbers.)
	4.0	Validation and Release Records	Document Release Records (There is a release record for each released version of each IT asset which includes Change Notice [CN] authority and positive evidence of validation.)
	5.0	Changes and Revision Records	Closed-loop Change process (A closed-loop and self-correcting process is used to release new information and to change information which is already released.)

Table 5 Assessment Phases and Requirements			
Phase	Category	Description	Requirement Example
Enabling System Requirements	6.0	Information Systems Architecture	As-Planned/As-Released Baseline for Information Systems (An as-planned and as-released baseline is used to maintain an up-to-date definition of the information systems and technology used by the enterprise.)
Interfaces to Core Requirements	7.0	Support, Operation and Maintenance	IT assets reviewed by cross-functional teams to determine need to upgrade (Are project managers coordinating requirements with Data, Records, Security, or using Configuration Boards of HCM or SCM teams to validate decisions to implement a change?)
	8.0	Human Resources and Training	CM function sufficiently staffed? (Are CM personnel trained?)
	9.0	Metrics and Continuous Improvement	Data gathering (Tools in place to gather data on the CM Process).

2.3.2 Checklists

Configuration Managers shall use authorized checklists to assure compliance with processes and assure consistency with quality of document reviews. Authorized checklists shall be maintained on the NCM website. Samples of Checklist are listed in Appendix 3. Checklists enable Configuration Managers:

1. To quickly identify concerns with a request.

2. To provide a standardized methodology for reviewing products.

3. To convey status on products.

4. To provide a summary of key areas that must be addressed at a minimum for a project or product to be accepted under formal CM.

2.3.3 Metrics

Configuration Managers will gather metrics on CM activities to assess and measure CM process performance for CIOs. They will prepare annual reports for NCM to review and consolidate for planning and implementing improvements to the CM process. The reports will cover the following classes of information.

1. For effectiveness of planning for and using CM.

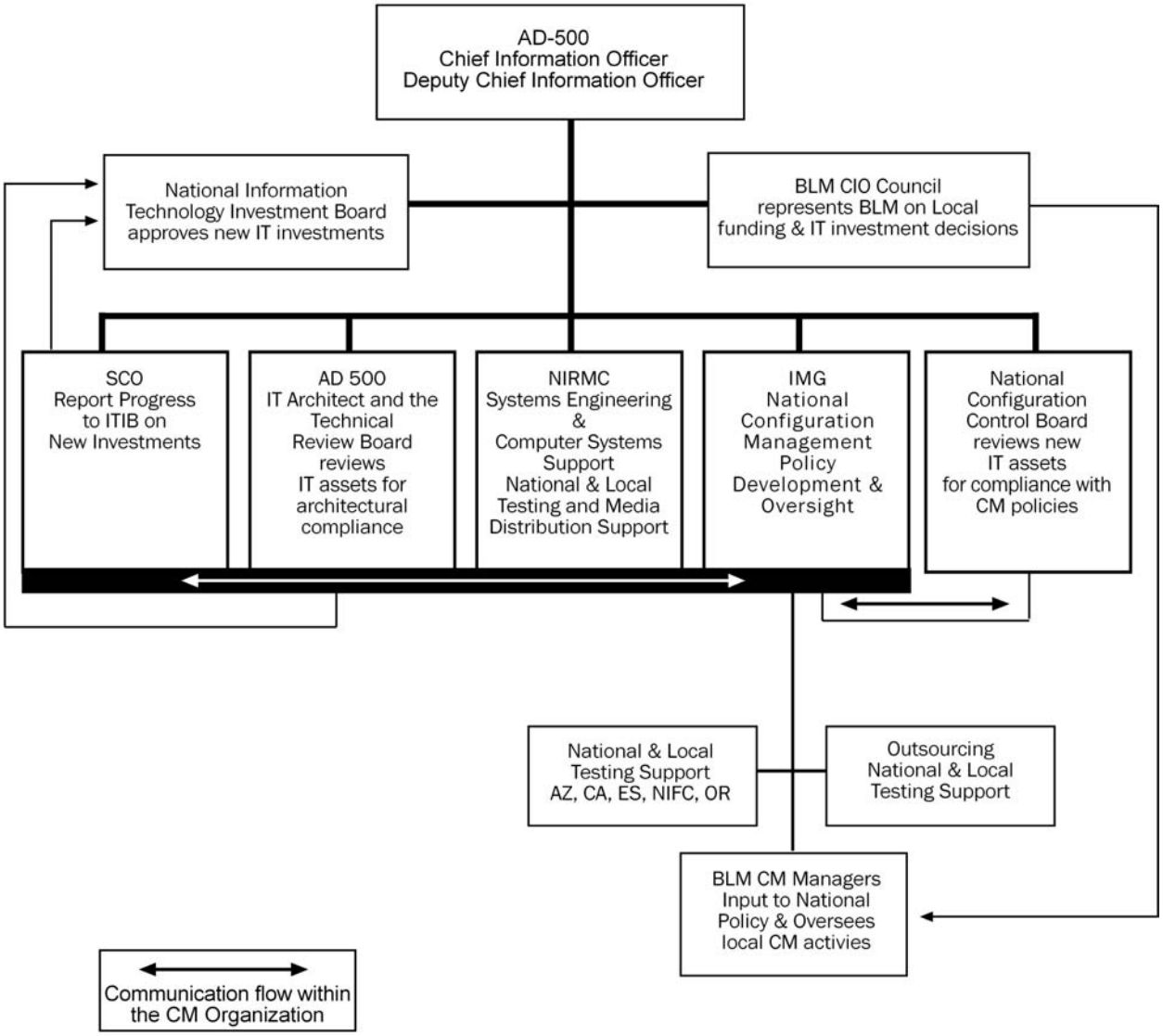
2. Providing a baseline for future projects to measure against.

3. Identifying deficiencies during the development phase and implementation phase of a project.

2.4 Organization

NCM responsibilities are within the IRM, Investment Management Group. NCM provides policy development and oversight of the BLM CM process. It is supported by NIRMC Systems Engineering for testing and by NIRMC Systems Support Division for software distribution. State and National Center CM offices are structured within varying levels of the organization, but report to their appropriate CIO. State and National Center Configuration Managers are members of the BLM's CM team to assist with policy development. Because the BLM's CM process capitalizes on decentralized supporting activities through the creation of virtual lines of operation, it is crucial that National, State, and National Center CM offices rely on Service Level Agreements (SLA), Statements of Work (SOW), and related contract mechanisms to accomplish supporting the BLM's CM process requirements for IT assets. Chart 1 describes the virtual lines of operation within the CM organization.

Chart 1 - National CM Organization



2.4.1 Configuration Boards

Boards or teams function to baseline documentation, validate, and verify the integrity of the information, and finalize application/software configurations prior to submitting IT assets for release. Board or team members are responsible for validating compliance with CM policy and procedures. Membership must include experienced CM, Data, IT Security, and Records personnel and subject matter experts.

BLM will use National, State, and National Center level configuration boards or teams to baseline final release of documentation and their associated application and hardware throughout their life cycle. This includes new software development activities and projects. For project level CM, project managers may use boards, teams, or perform the functions of the configuration board. In addition, project managers are expected to perform the following CM activities: configuration identification, configuration control, status accounting, audits and reviews. Project managers must manage, track, and document changes to their applications during development, acceptance, unit, integration, and system testing prior to releasing their final documentation and software to the National, State, or National Center level board. Project managers are not authorized to release an IT asset to BLM without the appropriate National, State, or National Center board concurrence or approval.

Under the direction of the CIO, the National Configuration Control Board (NCCB) reviews final release documentation for newly acquired IT assets or IT assets under the authority of the National Information Technology Investment Board (ITIB) to validate that the project complied with CM policy prior to releasing IT assets to the NCM baselines. The board's primary role is to maintain the integrity of NCM baselines by ensuring that IT assets are tested, documented, and coordinated with IT Security, Data, Records, Architecture, and system owners prior to granting approval to release to the NCM baselines. For existing IT assets, the NCM staff oversees final release to the NCM baselines and reports status to the NCCB. State and National Center level boards under the direction of their appropriate CIO inherit the national level role; however, they may expand their board's authority to include managing changes to existing IT assets or integrating their local CM board within their local ITIB board. Configuration Managers will ensure that all National, State, or National Center boards have charters that describe their purpose, objectives, and responsibilities. All chartered boards will have correlating operating procedures.

2.4.2 Testing Facilities

The BLM will use testing facilities and testers to document, conduct, and report test results on BLM's software and hardware IT assets. Testing shall be conducted at BLM identified testing facilities provided that they can meet the required test environment criteria. Although the National Test Lab (NTL) is the primary testing facility for national applications, NCM will use other BLM testing facilities to help with validation and release of national applications. NCM working with NIRMC will oversee the routing and scheduling of national applications to those facilities. This might include facilities in Arizona, California, Eastern States, National Interagency Fire Center (NIFC), and Oregon who has stated that they have test facilities. Testing of National, State, and National Center Level Applications may also be performed by approved off-site contractors when needed to fulfill the CM testing requirements. NCM will maintain a listing of those facilities approved to test national applications on their web site. State and National Center Configuration Managers are also required to maintain a listing of their approved testing facilities. Project managers must declare where testing will be conducted and identify those who will perform the testing in their draft master test plan. Moreover, all testing must be conducted at BLM NCM approved testing facilities.

Although testing may be done at approved testing facilities, all distributions and testing of national software and hardware will be coordinated through the NCM and NIRMC staff. NCM uses an electronic mail box at ncm@blm.gov to serve as a central repository for receiving CM documentation. The electronic mail box is monitored during core business hours by the NCM staff. State and National Center offices are encouraged to set up a similar electronic mail box for receiving State and National Center specific CM documentation and for distributing software and hardware.

2.4.3 BLM Configuration Management Team (BCMT)

BCMT serves as an integral partner in developing, shaping, and implementing the BLM CM process. They are responsible for coordinating all local issues and interfacing with NCM to manage national IT assets throughout BLM. Every State, National Center, and the Washington Office must have a designated Configuration Manager. The Configuration Manager is the source for receiving national software releases. They work with their CIO's and IRM Chiefs as

advisors to assist them with managing newly acquired and existing IT assets. The NCM coordinates all national software and hardware distributions through the BCMT.

2.4.4 Technical Review Board (TRB)

The CIO and the National ITIB established the TRB as a governance board to facilitate the ongoing development of the Information Technology Architecture (ITA) and to determine technical compliance with the technology layer of the Bureau Enterprise Architecture (BEA) for BLM's existing, planned, and future architecture. The board serves as the forum for adjudicating architectural compliance issues resulting from architectural project reviews prior to project presentation to the National ITIB related to national information systems and technology implementation.

The TRB reviews projects in the Select and Control Phase of the IMP for compliance to the ITA and the TRM. They prepare recommendations to the project to bring them into compliance. The TRB works closely with the National Configuration Manager to assure products scheduled for release to the national baseline comply with the ITA and that the Current Section of the TRM accurately reflects the NCM baseline. The National Configuration Manager or the NCCB is responsible for managing and releasing information to the NCM baseline.

2.4.5 Information Technology Investment Board

ITIBs are responsible for selecting, controlling, and evaluating all IT investments. There are chartered boards at the National, State, and National Center levels. At the national level, SCO oversees all projects with national scope; however at the State and National Center level, project oversight is handled through their CIO and State or NCCB or their Configuration Manager.

2.5 Change Management Process

The BLM will implement a CMP that is replicated throughout all levels of the organization. The process must identify who can make business decisions about IT assets and what IT assets are being placed under formal management. The CMP must be based on a standard set of procedures the BLM will use to ensure the integrity of its IT assets. Each CIO must ensure that a CMP similar to the national CMP is implemented within their jurisdiction and the process is communicated and followed.

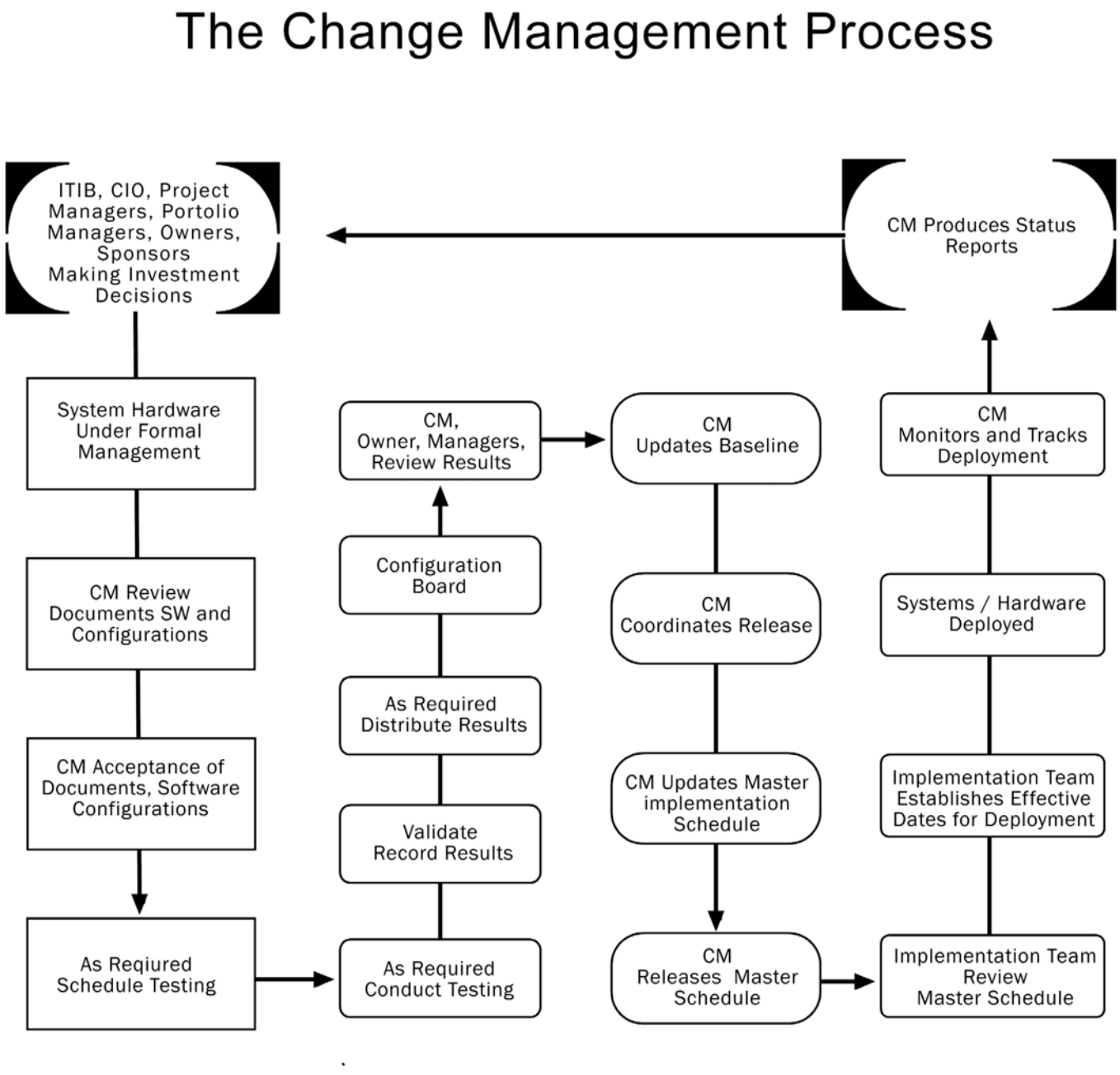
2.5.1 What is the Change Management Process?

The CMP documents the process for managing all IT assets placed under formal management. This includes all networked hardware, software, operating systems,

firmware, and COTS. A more extensive listing is under Section 2.5.6. The BLM will implement two tracks: standard and fast track. Standard track changes are complex and need to go before Configuration Boards. They usually represent newly acquired IT assets, but may also represent changes to existing IT assets. States and National Centers are encouraged to consult the SCO for guidance on thresholds. At the national level, all projects under review of the National ITIB follow the standard track, because they require NCCB approval; however, the National Configuration Manager may fast track changes for those IT assets that are fully documented and a part of the existing baseline. They are usually bug fixes or maintenance upgrade releases. At the national level, fast track changes do not require NCCB approval. Nonetheless, fast track changes like standard track changes still require test plans, test cases, CRs and decision documents.

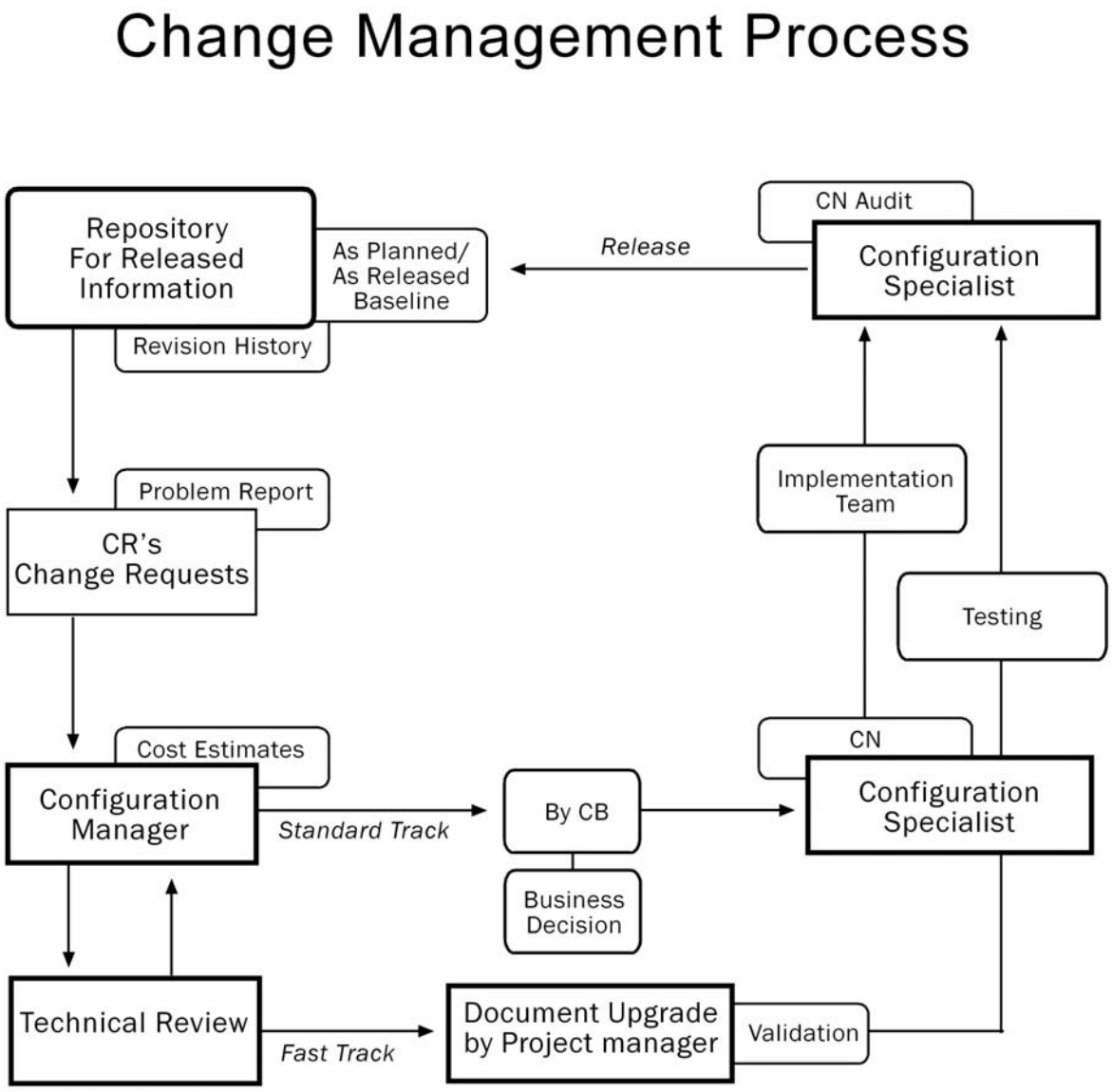
The BLM CMP begins with the approval to acquire an IT asset in the Select Phase of the IMP and the process runs throughout the Evaluate Phase. It is a close-loop process. Configuration Managers may fast track any existing IT asset that does not cause an expenditure of funds. System owners and project managers may request to fast track any existing IT asset; however, discretion is granted to the Configuration Manager or Configuration Board who manages the fast track process at the State or National Center level. Additionally, fast track priority processing is granted for those IT assets that have the greatest potential impact on BLM's network and desktop security. The following workflow diagram reflects the CMP.

Figure 1:


The Change Management Process
ITIB, CIO, Project Managers, Portolio Managers, Owners, Sponsors Making Investment Decisions
CM Produces Status Reports
System Hardware Under Formal Management
CM Review Documents SW and Configurations
CM Acceptance of Documents, Software Configurations
As Reqiured Schedule Testing
As Required Conduct Testing
Validate Record Results
As Required Distribute Results
Configuration Board
CM, Owner, Managers, Review Results
CM Updates Baseline
CM Coordinates Release
CM Updates Master implementation Schedule
CM Releases Master Schedule
Implementation Team Review Master Schedule
Implementation Team Establishes Effective Dates for Deployment
Systems / Hardware Deployed
CM Monitors and Tracks Deployment

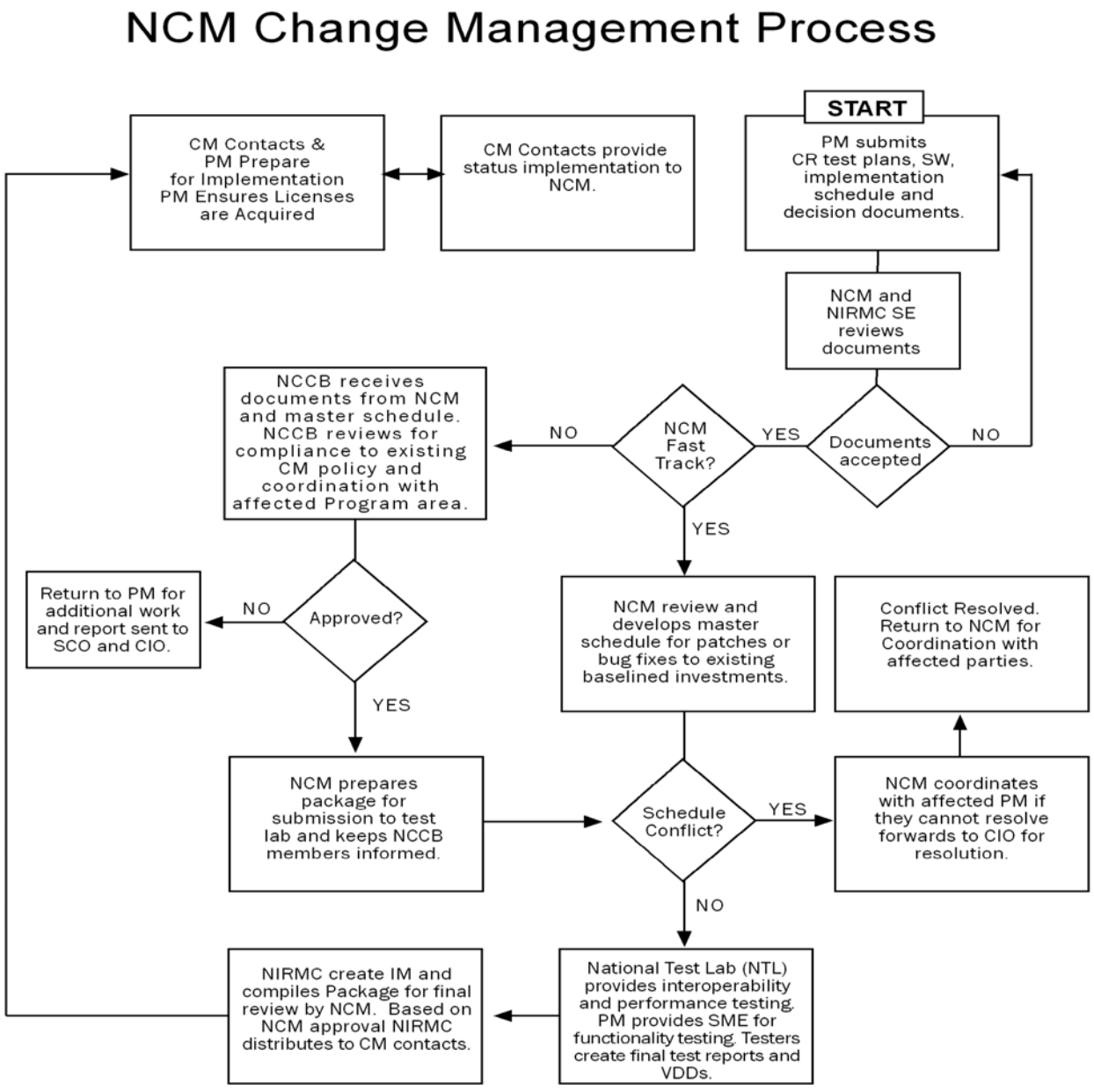
Additionally, the CMP is a closed-loop process. This process ensures that information about an IT asset is tracked, documented, and tested prior to updating the CM baselines. Key personnel involved are the project manager, National, State, or National Center Configuration Manager, appropriate Configuration Specialist, Systems Engineering (at the national level), and testers. The following relationship diagram reflects the CMP.

Figure 2



The following decision tree represents the National CMP. States and National Centers should implement a process similar to the national process.

Figure 3



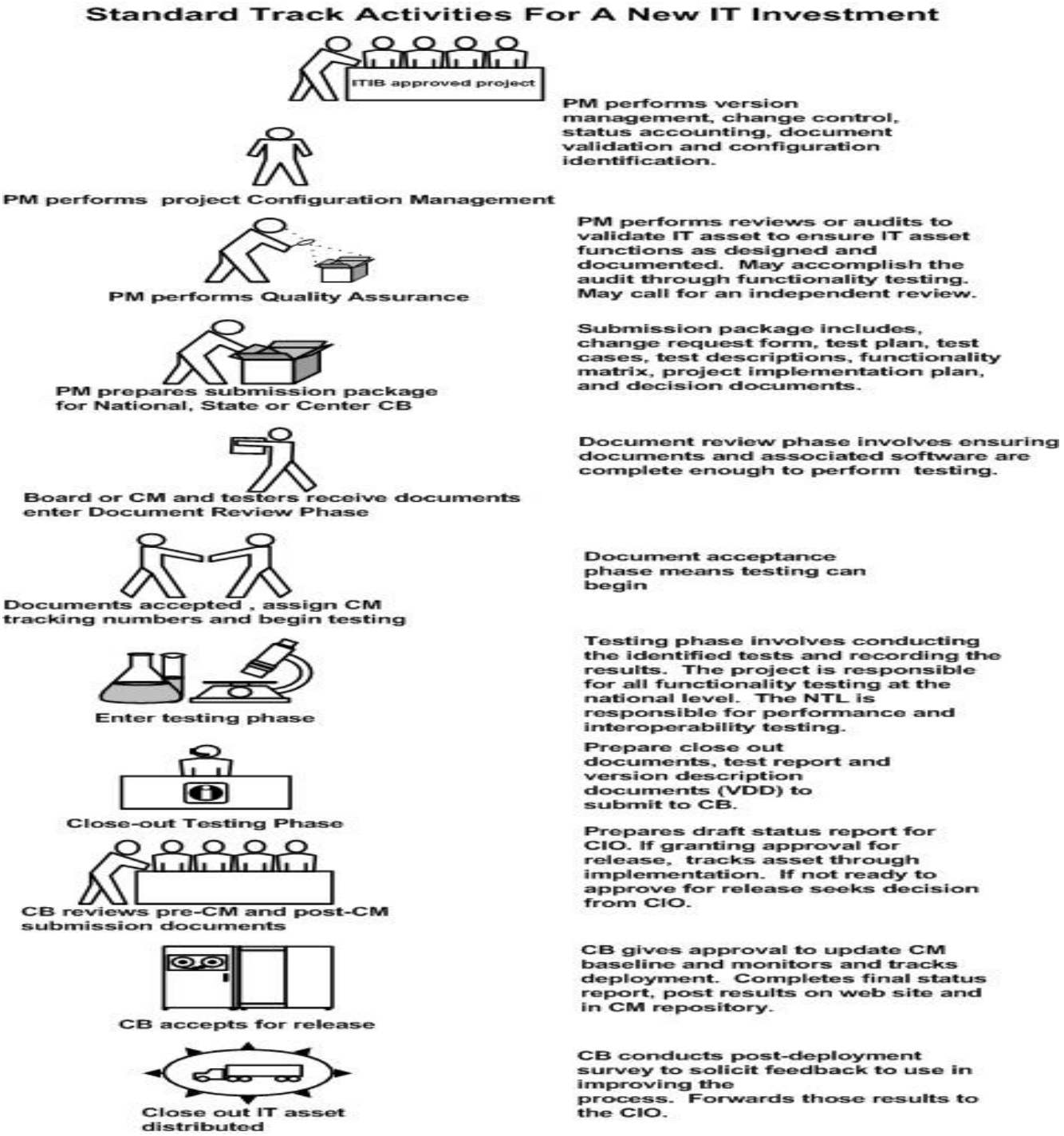
2.5.1.1 What are candidates for the standard track?

At the national level, any acquired IT asset that is new to the BLM must go through the standard track. State and NCCBs must identify those IT assets that must go through their standard track. A waiver may be granted for those COTS' assets determined by the CIO with the CIO Councils' advice to have low risk impact. Additionally, IT assets on the standard track may require additional reviews or more extensive testing to ensure compatibility with the architecture and the existing National, State, or National Center CM baselines.

What Activities Are Involved in Processing Standard Track Requests?

Please refer to figure 3 on the next page.

Figure 3

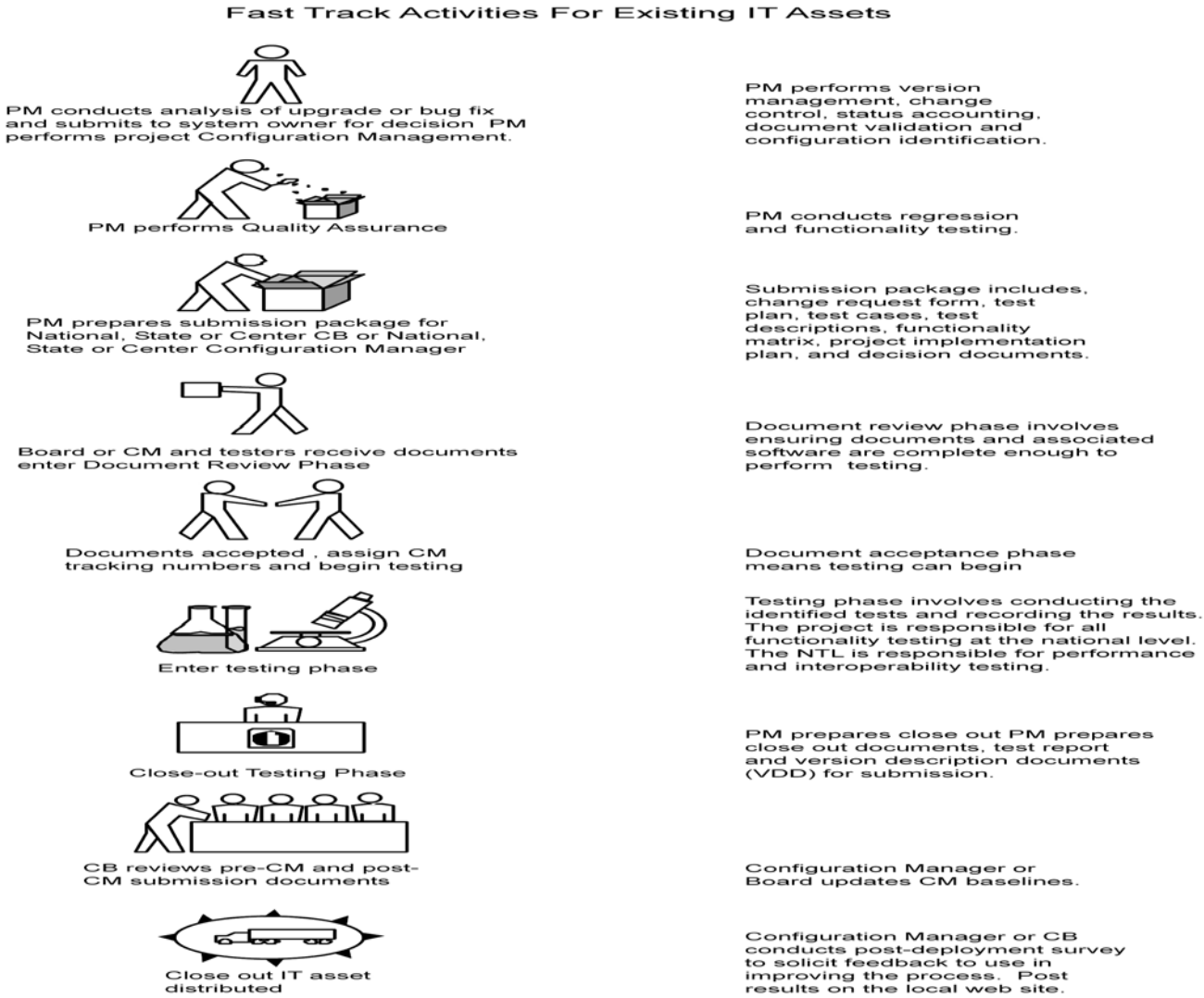

Standard Track Activities For A New IT Investment
ITIB approved project
PM performs version management, change control, status accounting, document validation and configuration identification.
PM performs project Configuration Management
PM performs reviews or audits to validate IT asset to ensure IT asset functions as designed and documented. May accomplish the audit through functionality testing. May call for an independent review.
PM performs Quality Assurance
Submission package includes, change request form, test plan, test cases, test descriptions, functionality matrix, project implementation plan, and decision documents.
PM prepares submission package for National, State or Center CB
Document review phase involves ensuring documents and associated software are complete enough to perform testing.
Board or CM and testers receive documents enter Document Review Phase
Document acceptance phase means testing can begin
Documents accepted , assign CM tracking numbers and begin testing
Testing phase involves conducting the identified tests and recording the results. The project is responsible for all functionality testing at the national level. The NTL is responsible for performance and interoperability testing.
Enter testing phase
Prepare close out documents, test report and version description documents (VDD) to submit to CB.
Close-out Testing Phase
Prepares draft status report for CIO. If granting approval for release, tracks asset through implementation. If not ready to approve for release seeks decision from CIO.
CB reviews pre-CM and post-CM submission documents
CB gives approval to update CM baseline and monitors and tracks deployment. Completes final status report, post results on web site and in CM repository.
CB accepts for release
CB conducts post-deployment survey to solicit feedback to use in improving the process. Forwards those results to the CIO.
Close out IT asset distributed

2.5.1.2. What are candidates for the fast track process?

Fast track changes are generally reserved for existing baselined IT assets, because they require less complex testing. Excellent candidates for the fast track process are IT COTS assets being upgraded to the latest version, and application bug fixes.

What Activities Are Involved in Processing Fast Track Requests?

Figure 4



2.5.2 Who Can Initiate Changes?

Anyone may initiate a change using the CR form. The CR form should be submitted to the local Configuration Manager and coordinated through the local CIO.

2.5.3 Who Can Authorize Changes?

Only management officials or their appointed representative identified in the IMP may authorize changes. Typically this consists of the local ITIB, CIO, sponsors, owners, portfolio and project managers under the direction of their Assistant Directors or State Directors.

Formal approvals are required to meet CM process objectives. Such approval is required regardless of the size of the development project, hardware system or its office of intended use (local office/unit use, statewide/center wide use, Bureau wide use). The granting of approval is evidenced by securing the appropriate signature(s) which constitutes approval to proceed. The withholding of approval, as evidenced by missing approval signature(s), constitutes a stop work order on the project until such time as the necessary approval is granted.

It is the responsibility of the reviewing official(s) or management officials to certify by his/her signature(s) that the goals, activities, and deliverables required for a particular phase within the IMP are met. Additionally, by the granting of his/her signature(s), the approving authority(s) is granting approval for the IT asset to continue into the next phase of the IMP.

2.5.4 How Are Changes Approved?

Approval to proceed is a management decision. It is based on an assessment of the progress of an IT asset within the IMP. The assessments, leading to either approval to proceed, stop work, redo some work are based on discussions between the project manager and the reviewing and approving official(s). Such discussions are geared to the goals, activities, and deliverables of the project that pertain to that particular phase in the IMP. Managers will base their assessments on a preestablished set of criteria and objectives identified in planning documents. Some things taken into account are as follows:

Impacts

Are sponsoring managers willing to provide resources in the development, testing, deployment, training, conversion, and maintenance for the full life of the proposed system?

Data

Have the data requirements been checked against national standards (Data Element Dictionary) or are they standard with your stakeholders, or other Federal, State, and local entities or constituency groups? Have the data already been collected (internally or externally)? And how was it collected?

2.5.5 Why Do We Manage Changes?

The BLM manages change to ensure that investment decisions are aligned with the BLM's Strategic Plan and assure that accountability for IT assets are appropriately managed, monitored, and tracked throughout their life cycle. Furthermore, it is BLM's implementation of the CM process that assures information about IT assets remains clear, accurate, up-to-date, and valid.

2.5.6 What Is Placed Under Formal Management?

Formal management does not mean under Configuration Board or CM control. It means there is a CMP that is documented, validated, and accessible to BLM end-users. The following IT assets are placed under formal CM control:

- Any software, applications, or operating system changes.
- Changes in the structure of national databases including fields, tables, etc.
- Hardware upgrades and new installs.
- Hardware, software, and application configuration settings.
- Released project documentation (user guides, system guides, test plans, test cases, test reports, VDDs, specifications, etc.)

Additional IT assets may be placed under CM control at management's discretion. Furthermore, CIOs must document the CMP for IT assets that impact CM baseline management. These IT assets should be placed under formal management. The following list identifies assets that impact CM baselines:

- Any IT asset acquisition
- Enhancements to web pages
- SOPs
- Administrative and technical procedural changes

- IT Manuals and Handbooks
- Technical Reference Model

2.5.7 Document Management

National, State, National Center, and Project level Configuration Managers or Configuration Boards will manage documents and changes to documents that affect CM baselines. All documentation will be validated before it can be released. Validation means the end-users, and subject matter experts have reviewed the documents to ensure they meet the requirements of the higher level documents from which they were derived. This includes test plans, test cases, test descriptions, project implementation schedules, VDDs, test results, user guides and other associated documentation affecting system use. Document management also includes managing revisions. Initial releases of all CM forms must reflect the revision number A in the footer. Subsequent revisions proceed in alphabetical order. Other CM documentation will use a numeric scheme starting with 1.0. The creator of the document assigns the revision number and is responsible for submitting the document to CM for formal management. The CM manager ensures that all documents affected by the change are scheduled and updated.

2.5.8 CM Tracking and Document Numbering

The BLM formerly implemented an alphanumeric CM tracking numbering scheme that allowed for unique numbering. This practice remains in effect until superceded by an automated system. Each National, State, National Center, and the Washington Office will generate tracking numbers for CM documentation according to this numbering scheme. No document will be placed under formal CM control without a tracking number. CM tracking numbers will be placed in the left footer of the document. This scheme prevents duplication of numbers between offices. CM tracking numbers will be managed by the local Configuration Manager. The following CM tracking number represents this numbering scheme. Each field is separated by a dash, and a sample number would reflect:

A-BB-CCC-DDD-EEE-VX.00.00-MMDDYY

A – Reserved for National Level

BB – Reserved for State, National Center, Office level code

CCC – System Designator Code

DDD – Computer Software Configuration Item (CSCI)

EEE – Document Type

VX.00.00 – Version Release Number

MMDDYYYY — Date Baselined

National Level Designator

The first field is a single alpha character, used for documents under NCM. If the document is not under NCM, this field is left blank represented by an X.

State, National Center, or Office Level Designator

The second field is two alpha characters in length, coded with the 2 letter office code. This shows who owns the document. If National owns the document this field is left blank represented by XX.

System Designator Code

The third field is three characters in length providing the applicable system code. If only one or two characters are used as the system code, the proceeding or left most characters are blank fields represented by the code X. This code is obtained from the BLM corporate metadata repository (CMR).

Computer Software and Hardware Configuration Item Designator Code

The fourth field is three alpha characters in length and identifies the CSCI, Hardware Configuration Item, Administrative Configuration Item or Product Configuration Item for the document. CSCI designators are assigned by the National Configuration Manager for National Systems and by the State or National Center Configuration Manager for their systems. CSCI designators are coordinated through the National Configuration Manager.

.

Document Type

The fifth field is three alpha characters in length and identifies the type of document.

CM Configuration Management
CMP Change Management Process
CN Change Notice
CR Change Request

HRS Hardware Requirements Specification
IDD Interface Design Document
IRS Interface Requirements Specification
RDD Requirements Definition Document
RSL Requirements Summary List
RTM Requirements Traceability Matrix
SDD System Design Document
SPS Software Product Specification
SRC Source Code
SRF Support Request Form
SRS Software Requirements Specification
STD Software Test Description
STP Software Test Plan
VDD Version Description Document

Version Release Number

The sixth field is six alpha numeric characters in length and identifies the product release number.

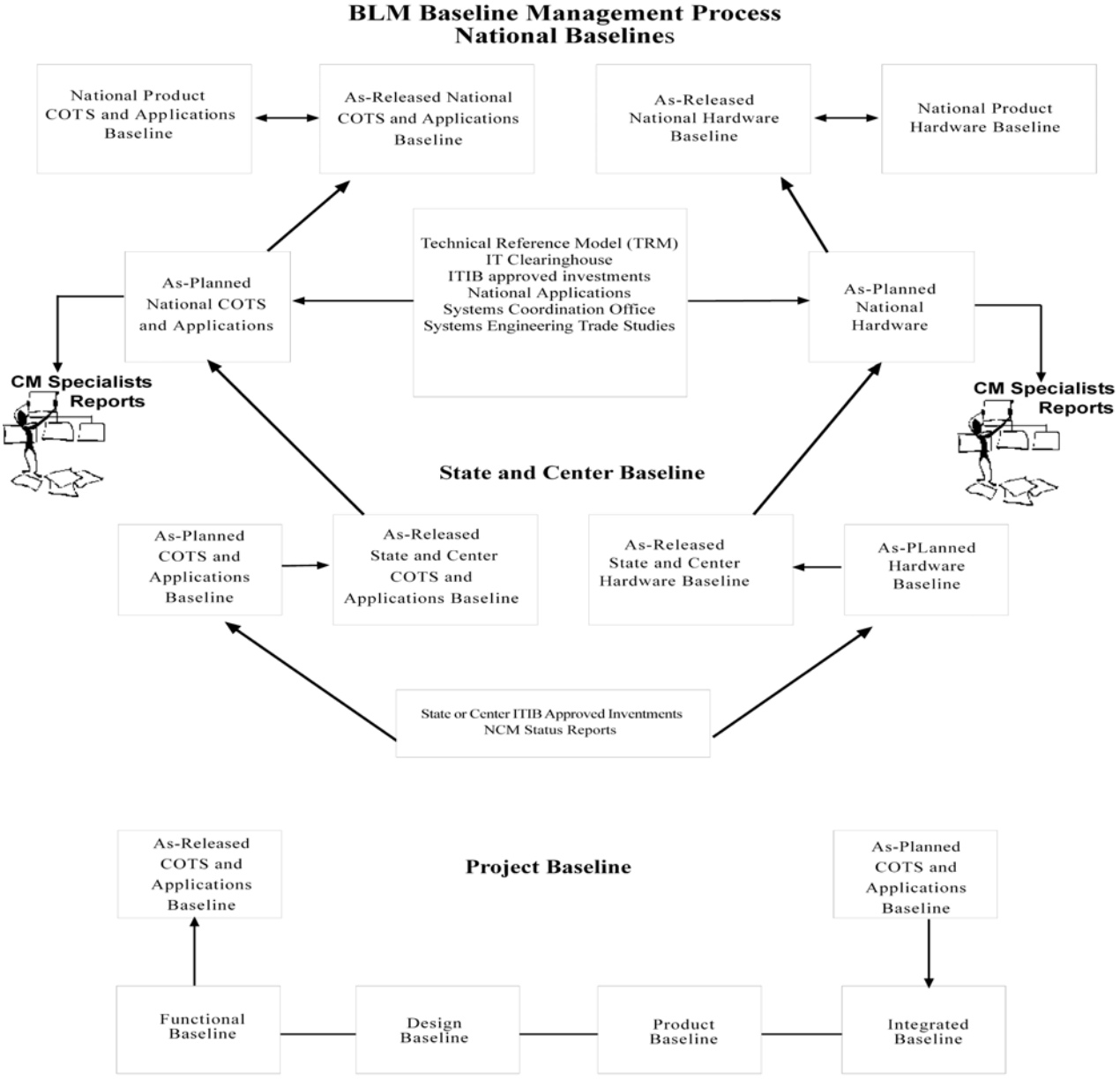
Baseline Date

The seventh field is eight numeric characters in length and represents the date Configuration Manager certifies IT asset for release. The date is reflected in mmddyyyy format.

2.5.9 Baseline Management Process

CM baselines are managed by Configuration Managers, National, State, National Center, and Project Level Configuration Boards. Baseline management includes version management, reviewing releases of applications, COTS, middleware, hardware, and telecommunications devices for opportunities to consolidate or standardize IT assets and reporting and coordinating those efforts. At the national level, it also includes monitoring Systems Engineering trade studies, the IT Clearinghouse or its designated replacement system, and the CMP to create the national As-Planned Applications and COTS CM baseline. The As-Released Applications and COTS CM baseline is created once the IT asset is ready for release to BLM. State, National Center, Project Managers, and Portfolio Managers should monitor the As-Planned Applications and COTS CM baseline to assist with their planning efforts. Information included on CM baselines reflects targeted implementation date, application name, software configuration, platform, and system requirements. The following relationship diagram demonstrates the hierarchy of CM baselines.

Figure 5



Projects are done at the National, State and Center levels. Some typical project CM baselines include, functional, design, product and integrated baselines. These baselines flow into the projects As-Planned CM baseline and their As-Released CM baseline flows into the appropriate National, State and Center As-Planned CMBaseline.

2.5.10 Library Control

The NCM, State, or National Center CM document libraries and media repositories will be maintained by the appropriate CM Specialist. CM libraries and media repositories shall include all CM documentation needed to release an IT asset to CM baselines. CM documentation and media shall be maintained in secure, fireproof storage. Project libraries shall maintain copies of all project documentation including that submitted to the National, State, or National Center Configuration Manager. All records (documentation and media) shall be retained and disposed of according to existing Records policy. Additionally, the CM Specialist will maintain check in and check out logs establishing a clear chain of custody for document and software releases. The log will be maintained both electronically and manually. A paper copy will be displayed outside of the filing cabinet for review. The CM Specialist will perform monthly audits to provide status accountings on all documentation and media maintained in the library and media repository.

2.6 Managing Acquisition CM

According to the IMP, proponents are responsible for securing sponsors and the sponsor is responsible for assigning a project manager. It also states that the sponsor may become the system owner. The IMP also require the proponent or Project Manager to create an acquisition plan. An outline of the acquisition plan is included in Section 3 and instructions for completing the plan are included in the Best Practices Section in Appendix 2. The CM process requires the proponent to consult the appropriate Configuration Manager to ensure the IT asset proposed to meet the business need, does not currently exist within the BLM, and it does not conflict with the CM planned or released baselines. Once the Project Manager receives approval to proceed, the Configuration Manager should be included in subsequent planning to ensure appropriate language is added to contracts. NCM will publish language examples on their web page. Meanwhile, typical language might include:

> ***The contractor shall use the IEEE standard for documentation to comply with the BLM CM process. As a part of acceptance testing, the contractor shall test their product against the BLM-CONFIGURED baseline.***

CM managers shall also be included and consulted in the review phase for developing hardware and software requirements. The document created prior to acquisition is known as the requirements definition document (RDD). It establishes the operational framework and performance baseline for the IT acquisition. The RDD becomes the As-Planned baseline at the investment decision to acquire the asset.

The RDD is the primary force driving the search for a realistic and affordable solution to mission need during the Select Phase. The initial RDD is developed early in the IMP by the sponsoring program. It translates the "need" in the Mission Need Statement into initial top level requirements addressing such concerns as performance, supportability, physical and functional integration, human integration, IT security, data, IT architecture, test and evaluation, implementation and transition, quality assurance, configuration management, and implementation. The RDD must *not* describe a specific solution to mission need, and should not preclude leasing, commercial, or non-developmental solutions. In the Select Phase, these initial requirements are evaluated against the cost, benefits, schedule, and risk of various candidate solutions and brought into balance with an affordable solution.

At the investment decision, the RDD defines the operational concept and requirements the approved acquisition is intended to achieve. It is the basis for evaluating the readiness of resultant products and services to become operational. Sponsor requirements not included in the RDD at the investment decision are returned to the sponsoring line of business for disposition. The Assistant, State, or National Center Director business program with the mission need approves the RDD and all changes to it.

NOTE: The RDD is NOT a design specification; it contains only top level requirements.

DISTRIBUTION

The sponsor must distribute copies of the approved RDD to the appropriate Configuration Manager.

2.7 Managing Hardware CM

The BLM will use the most cost-effective means to acquire IT assets. This includes, but is not limited to, consolidating hardware purchases when appropriate to increase its buying power and to achieve the maximum return on its investment. The BLM will manage servers, desktops, laptops, radios, cell phones, and associated software and firmware to achieve support efficiencies. Table 6 describes HCM activities.

Table 6 - Managing Workstations, Servers, Routers, Radios, and Telephony Equipment for Infrastructure Replacement, and Product Upgrades

HCM Team or Integrated Project Team (IPT)	Product	Approval Authority
Configuration Manager	As-Planned Hardware Product Baseline	CIO
System Engineer		
System Administrator		

Table 6 - Managing Workstations, Servers, Routers, Radios, and Telephony Equipment for Infrastructure Replacement, and Product Upgrades		
HCM Team or Integrated Project Team (IPT)	Product	Approval Authority
Email Administrator		
Network Administrator		
Help Desk Lead		
User Representative		

Description:

The HCM Team under the direction of the CIO and business process owners develops, approves, and manages configuration requirements for the hardware. The team requests machines with corresponding firmware and operating systems to evaluate. The team documents requirements in test plans, test cases, and test descriptions. The documents form the foundation of the As-Planned Hardware Product Baseline. Many of the CM activities conducted during requirements definition for the currently fielded capability are replicated to assure smooth transition and continuity of operational service as installed equipment is modified and upgraded.

Maintaining HCM

1. The team generates test plans to test out hardware platforms against approved software baselines.
2. The team evaluates hardware platforms and forwards recommendations to the CIO for technical approval to the baseline.
3. The CM Specialist verifies the logs for the configuration items, updates them as appropriate and notifies the Configuration Manager for release of the information to the baseline.

2.8 Managing Software CM

All software development projects will follow the IEEE Software Life Cycle Process Standards IEEE/EIA Std. 12207.0-1996 standard for documenting BLM software and applications. NIRMC Systems Engineering and the NCM staff tailored the IEEE guidance and best practices to meet BLM's software development and applications needs. The BLM's best practices, samples of plans, templates, forms, and checklists are included in Appendices B through E within this Handbook and they are also posted on the National CM web site. All BLM staff responsible for developing and maintaining software applications for IT assets must comply with the documentation standards based on the below listed IEEE standards:

- Standard for Software Configuration Management Plans; IEEE Std. 828-1998,

- The guide to Software Configuration Management; IEEE Std. 1042-1987,
- Standard for Software Test Documentation; IEEE Std. 829-1998,
- Recommended Practice for Software Requirements Specifications; IEEE Std. 830-1998,
- Recommended Practice for Software Design Descriptions; IEEE Std. 1016-1998,
- Standard for Software User Documentation; IEEE Std. 1063-1987,
- The guide for Developing System Requirements Specifications; IEEE Std. 1233, 1998 Edition and,
- Guide for Information Technology-System Definition-Concept of Operations Document IEEE Std. 1362-1998.

The declaring of a single software development standard is a departure from earlier policy that allowed BLM developers to choose their CM methodology. Each configuration manager must acquire a copy of the standard for their reference library. Each project manager must complete a Software Configuration Management Plan. It may be a part of the project plan or presented under separate cover. This plan documents what SCM activities are to be done, how they are to be done, who is responsible for doing specific activities, when they are to happen, and what resources are required. The sponsor may tailor the plan in the areas of SCM activities and SCM resources for non-mission critical software activities; however, the sponsor may not tailor the plan for mission critical systems. Please refer to Chapter 3 for a detailed description of the SCM Plan. Table 7 describes SCM activities.

Table 7 - Managing Software Development Activities and COTS

SCM Team (IPT)	Product	Approval Authority
Configuration Manager System Engineer System Administrator Application Developer Network Administrator Help Desk Lead User Representative	As-Planned COTS and Application Baseline **Documents Required** System Design Document, Functionality Matrix, Decision Documents	CIO

Table 7 - Managing Software Development Activities and COTS		
SCM Team (IPT)	Product	Approval Authority
Description: The SCM Team under the direction of the CIO and business process owners develops, approves, and manages configuration requirements for the software asset. The team documents requirements in test plans, test cases, and test descriptions. The documents form the foundation of the As-Planned Software Product Baseline. Many of the CM activities conducted during requirements definition for the currently fielded capability are replicated to assure smooth transition and continuity of operational service as installed software is modified and upgraded. Project Managers are expected to conduct internal reviews to report their findings to the systems owner, sponsor, and appropriate CIO and ITIB. Internal reviews may be verified through the customer's functional testing. Project Managers may conduct a functional configuration audit (FCA) or a physical configuration audit (PCA). Project Managers may refer to the IEEE standards for audits.		
Maintaining SCM 1. The team evaluates new releases and forwards recommendations to the system owner and CIO for approval to proceed. 2. The team generates test plans to test products against approved software baselines. 3. The Configuration Manager assigned handles change management for the project. 4. The CM Specialist verifies the logs for the configuration items, updates them as appropriate and notifies the Configuration Manager for release of the information to the baseline. 5. Asset undergoes testing for release to the baseline. 6. Product performs as expected, results recorded 7. Software As-Released Baseline is Updated.		

2.9 Testing Activities

The BLM application developers of National, State, National Center, or Office-wide systems must use testing facilities approved by the NCM office. The NTL in Denver is the primary facility for testing performance and interoperability of national applications. For alternative test sites to be approved, they must be able to demonstrate that they can meet the same software engineering test or system engineering testing environment as the NTL. All personnel assigned to the testing facilities must complete requirements' definitions, test planning, and development training Testers assigned to each Lab must use the same criteria established for testing as the NTL.

System owners or project managers are responsible for identifying and providing testers for their systems in the test plan. These testers are responsible for acceptance, usability, regression, and system (functionality) testing. Teams should consists of BLM subject matter experts.

For instance, the make up of an HCM team should include members in Table 8.

Table 8 - Testing Hardware

HCM Testing Team (IPT)	Product	Approval Authority
Test Configuration Manager	As-Released Hardware Product Baseline **Documents Required** Test Descriptions, Test Cases Test Plans, and Test Results	Sponsor or designated representative
Test Director		
Project Configuration Manager		
System Engineer		
System Administrator		
Network Administrator		
Help Desk Lead		
User Representative		

Description:

The purpose of testing is to establish whether performance and functional requirements defined in the Functionality Matrix are achieved or are not achieved. Testing also establishes whether the system documentation is accurate. The Project Team Configuration Manager manages changes to test configurations. The HCM team will perform testing according to the test documents. The test director will coordinate testing with the HCM team.

A typical software team should include members shown in Table 9.

Table 9 - Testing Software		
SCM Testing Team (IPT)	Product	Approval Authority
Test Configuration Manager Test Director Project Configuration Manager System Engineer System Administrator Network Administrator Application Developer User Representative	As-Released Application Baseline **Documents Required** Test Plan, Test Cases, Test Report, System Acceptance Checklist User Acceptance Checklist, User Guide, System Guide, Implementation Plan	Sponsor or designated representative
Description: The purpose of testing is to establish whether performance and functional requirements defined in the Functionality Matrix are achieved or are not achieved. Testing also establishes whether the system design is validated and documented. The Project Team Configuration Manager manages change to test configurations. This applies to both developmental and operational test and evaluation. For National assets, the National Configuration Manager coordinates integration and interoperability testing.		

2.10 Establishing Testing Priorities

The NCM staff reviews project plans and decision documents to schedule tests through the identified testing facility. When a conflict in a schedule arises, the National Configuration Manager will contact the affected parties to reach a decision. If a decision cannot be reached, it will be elevated to the CIO or their designated representative for resolution. State and National Center CIO's may delegate this authority to State and National Center Configuration Managers or their Configuration Boards. The National Configuration Manager schedules testing based on a tiered system: priority level, risk level to the bureau, complexity (class of problems), and completeness of documentation. Priority levels are as follows:

Priority 1 Urgent determined by BLM Systems having the greatest potential impact to the BLM-wide population.

Priority 2 Fast track usually reserved for existing systems.

Priority 3 Standard track usually reserved for new systems under ITIB review because of complex coordination requirements.

High Risk is assigned to software and application systems that pose security risks, threaten security of financial data or may compromise the network infrastructure (servers, routers, and desktop systems). High risk may cause a rescheduling of other activities within the lab. The system will not operate until the problem is resolved. There is no work around available. Resolution is required immediately. These problems will be resolved according to the fast track process

Medium Risk is existing software and applications undergoing upgrade, bug-fixes. Production or progress can proceed but with major impact on the integrity and timeliness of the system. May cause delays to schedule and impact costs.

Low Risk is assigned to new applications and COTS software under the ITIB, because they are undergoing evaluation, and testing and need approval from the ITIB after completion prior to deployment, or production or progress can proceed with minimal impact on system integrity and timeliness. This includes any problem report classified as a I or II that a work around exists.

Classes of Systems

Class 1 BLM National Systems

Class 2 Departmental Systems

Class 3 Multi-use State Systems

Class 4 Statewide systems

Class 5 Office systems

Class 6 Group systems

Within each category, testing is also scheduled on a first come first serve basis. States and National Centers will follow NCM priority guidance for testing systems. Ultimately, scheduling systems for testing on this tiered system complements business needs identified in the decision documents.

H-1268-1 Bureau of Land Management
Configuration Management Handbook

Chapter 3 - Documentation

3.0 Documentation

This chapter describes the forms, templates, and documents included in the CM Process. Project Managers and other trained IT professionals must complete and submit a CR, SRF, Test Plan, Test Descriptions, Project Implementation Schedule, and Decision Documents to CM to schedule interoperability and performance testing prior to deploying national systems. Documentation must be submitted in sufficient time to correct any deficiencies that may delay scheduling the tests. Project managers of new IT assets should allow at least 6 to 8 weeks to coordinate, review and fix deficiencies in the documentation; however, they should allow at least 2 to 4 weeks for existing IT assets. Testing can only begin when requirements are clearly documented for setting up the testing environment and the project manager has identified the tests to be conducted, and the subject matter experts for consulting on applications and in some cases performing the tests. State and National Center CM offices must use the established CM forms and associated documents to manage changes to IT assets.

3.1 Forms

All forms for use within the CMP shall be created in accordance with existing records management policy. Samples of all CM forms, templates, and documents shall be maintained on the NCM website.

3.1.1 Change Request (CR)

The CR replaces the Request for Change Proposal (RCP) previously used by NCM. The CR will be used to initiate changes to all IT assets identified for formal management including the associated documentation. All employees will use the CR to request changes. National, State, and National Center Configuration Managers will manage the CR. Some reasons for submitting a CR are reflected below:

Application Bug Fixes

If a product is identified as requiring an application bug fix that is necessary to correct a known or unknown problem, then it must be documented with a description of the problem and how it impacts the current environment within BLM special processing outside of the normal procedures.

Vendor Requirement

If a vendor identifies a problem with their COTS product requiring a patch to correct a known problem that affects Security, Data, or functionality, it must be documented on a CR by the owner, sponsor, or their project manager and submitted to the Configuration Manager for processing.

Processing the Change Request

1. Configuration Manager or Configuration Board members review CR to decide if CR was coordinated through CIO, sponsor, or system owners. If coordinated and all approvals are there, Go to Step 2. If CR was not coordinated properly, then return to requester for proper coordination.

2. Configuration Manager or Configuration Board members decide if the IT asset can be fast tracked. If fast tracked, Go To Step 4, otherwise go to Step 3.

3. Configuration Manager or Configuration Board members reviews CR, assesses for meeting requirements and prioritizes.

4. CM staff updates the master schedule of all IT assets in NCM informing all affected parties.

5. CM staff submits documents to testing.

6. Testing completed. CM staff notifies affected parties.

7. Affected parties review results.

8. Results are finalized, documented, and released in Test Reports, VDDs, and Status Reports to affected parties.

3.1.2 Change Notice (CN)

All Configuration Managers will use this form to track and monitor changes to existing and new IT assets. The CN form is designed to function as a historical record of changes and is integrally linked to the CR. No other form will be used to track changes. This form is reserved for CM staff only which includes

National, State, National Center, and Project Level Configuration Managers and Configuration Specialists.

Processing the Change Notice

1. Configuration Manager or Configuration Board members review CNs to decide if CN identifies all documents and systems affected by the proposed change. If CN is complete, Go to Step 2. If CN is incomplete, then return to the appropriate Configuration Manager (Project Level or State/National Center personnel).

2. Configuration Manager or Configuration Board members records status of the associated CR on the CN form to provide system owners progress on configuration items impacted by the change in a single form. Go to Step 3.

3. Release CN to appropriate testing facility to implement change.

3.1.3 The Problem Report (PR)

Currently, BLM uses the National Help Desk System to report application and hardware problems. The PR will be used to identify those IT assets that may require patches, upgrades, or system enhancements. The PR may be used to generate a CR.

Processing the Problem Report to Produce a CR

1. Help Desk personnel should provide a report to the CIO on Help Desk tickets. Upon review of the tickets, the CIO may send the report to the appropriate Configuration Manager for coordination. Go to Step 2.

2. The Configuration Manager or Configuration Board members review the report and contacts system owner to decide if a CR is needed. If CR is needed, then Go to Step 3. If system owner and board decides a CR is not needed, then file documents according to Records Management procedures.

3. System Owner or project manager generates CR. Go to Step 4.

4. Configuration Manager or Configuration Board members decide if the IT asset can be fast tracked. If fast tracked, go to Step 5, otherwise return to requestor for additional information.

5. Configuration Manager or Configuration Board members reviews CR, assesses for meeting requirements and prioritizes. Go to Step 6.

6. CM staff updates the master schedule of all IT assets in NCM informing all affected parties

7. CM staff submits documents to testing

8. Testing completed. CM staff notifies affected parties.

9. Affected parties review results.

10. Results are finalized, documented, and released in Test Reports, VDDs, and Status Reports to affected parties

3.1.4 Support Request Form

The SRF replaced the Test Lab Request Form. The SRF is used to document software and hardware requirements and the testing environment. All test labs identified to work with National, State, and National Center applications will use this form to record and track and setup the environment for server, workstation, and network requirements for testing.

3.1.5 Deviations and Waivers

Deviations and waivers are granted when the proposed application, system, or hardware product meet future architectural guidance. A request for deviation, once approved, is authorization to depart from a particular performance or design requirements of a specification, drawing, or other document for a specific number of units or period of time. A request for waiver, once approved, is a formal permanent change to the requirements. Deviations and waivers are submitted to the appropriate Configuration Manager for resolution. They may be submitted in electronic mail. Deviations and waivers must address the classes of information described in Table 10.

Table 10	**Deviation and Waivers**
Class of Information	Description
Introduction	Describes the reason for the request,
Impact Statement	Describes the effect for the BLM, if not granted.

For national level systems, deviations and waivers are approved or disapproved by the BLM CIO or the Deputy CIO. State and National Centers should use a similar process.

3.2 Plans

Samples of all plans needed to release IT assets are located on the NCM website.

3.2.1 Software Configuration Management Plan

A CM approach will be described in the project plan to include IT Security, Records, and Data. The approach should be outlined in sufficient detail to address the Bureau's requirements. This includes for both hardware and software IT assets. The project plan is a deliverable under the IMP. The SCM plan must address the following classes of information described in Table 11.

Table 11	**SCM Plan Items**
Class of Information	Description
Introduction	Describes the Plan's purpose, scope of application, key terms, and references.
SCM Management	(Who?) Identifies the responsibilities and authorities for accomplishing plan activities.
SCM Activities	(What?) Identifies all activities to be performed.
SCM Schedules	(When?) Identifies the required coordination of SCM activities.
SCM Resources	(How?) Identifies tools and physical human resources required for execution of the Plan
SCM Plan Maintenance	Identifies how the Plan will be kept current while in effect.

3.2.2 Software Acquisition Plan

The BLM's IMP requires a software acquisition plan for both COTS and custom-COTS product. COTS products are not excluded, although they are generally considered as stable and are normally well-defined in terms of documentation and known capabilities and limitations. The plan should be outlined in sufficient detail to address the Bureau's requirements. The Acquisition Plan (AP) must address the following classes of information described in Table 12.

Table 12 AP Items	
Class of Information	Description
Introduction	Describes the Plan's purpose, scope of application, key terms, and references.
AP Management	(Who?) Identifies the responsibilities and authorities for accomplishing plan activities.
AP Activities	(What?) Identifies all activities to be performed.
AP Schedules	(When?) Identifies the required coordination of SCM activities.
AP Resources	(How?) Identifies tools and physical human resources required for execution of the Plan
Acquisition Plan Maintenance	Identifies how the Plan will be kept current while in effect.

3.2.3 Master Test Plan (MTP)

The Project Manager develops a draft Master Test Plan (MTP) in the Select Phase of the IMP. NIRMC Systems Engineering will review and evaluate all MTPs for national applications in the Select Phase prior to a project moving into the Control Phase of the IMP. State and National Center applications will be reviewed by subject matter experts. The draft MTP is a deliverable and is used for documenting all testable requirements. Procedures for completing MTPs are posted on the NCM website. Only BLM authorized test personnel as identified in test plans are authorized to conduct testing. Testers are responsible for preparing the VDDs, and Test reports.

The MTP must address the following classes of information described in Table 13.

Table 13 MTP Items	
Class of Information	Description
Introduction	Describes the plan's purpose, scope of application, key terms, and references.
MTP Management	(Who?) Identifies the responsibilities and authorities for accomplishing plan activities.
MTP Activities	(What?) Identifies all activities to be performed.
MTP Schedules	(When?) Identifies the required coordination of MTP activities.

Table 13	MTP Items
MTP Resources	(How?) Identifies tools and physical human resources required for execution of the plan.
MTP Maintenance	Identifies how the plan will be kept current while in effect.

3.2.4 Transition/Deployment Plan (Implementation Planning)

A Transition/Deployment plan or the project implementation schedule will be submitted to the CM staff to assist with coordinating and prioritizing testing for release. The Transition/Deployment plan is a deliverable under the IMP. The Transition/Deployment plan must address the following classes of information identified in Table 14.

Table 14	Implentation Plan (IP) Items
Class of Information	Description
Introduction	Describes the plan's purpose, scope of application, key terms, and references.
IP Management	(Who?) Identifies the responsibilities and authorities for accomplishing plan activities.
IP Activities	(What?) Identifies all activities to be performed .
IP Schedules	(When?) Identifies the required coordination of IP activities in the project.
IP Resources	(How?) Identifies tools and physical human resources required for execution of the plan.
IP Maintenance	Identifies how the Plan will be kept current while in effect.

3.3 Decision Documents

Decision documents can be electronic mail, signed checklists, or formal letters that establish the audit trail and connect IT assets to their business owners. Sample decision documents and templates will be located on the NCM website.

3.4 Requirements Definition Document

The initial RDD establishes the high level requirements. After acceptance and approval, the RDD can be transformed into the functionality matrix. The RDD must address the following classes of information described in Table 15.

Table 15 Requirements Definition Document	
Class of Information	**Description**
Signature Page	Include: the title "Requirements Definition Document" and name of the acquisition program; signature of the Sponsoring Authority within the Directorate or Program Area with the mission need and signature date; name, organizational code, phone number, and FAX number of the point of contact (POC) for the RDD.
Table of Contents	List sections, subsections, and other elements in the RDD and provide the page number.
Background	Briefly describe the mission need and how the proposed capability will satisfy the need. Describe any substantive changes to the RDD since the Investment Decision, and explain why the changes were needed.
Operational Concept	Briefly describe the operational environment and intended service life for the required capability. Include how it will be used in the operational environment, and how it will affect users. Define hardware and software maintenance requirements. Quantify the total number of units or scope of services that are required. Define any schedule constraints
Technical Performance	Define operational and functional requirements the new capability must provide to satisfy mission need. Define product characteristics and performance requirements.
Functional Integration	Define functional integration requirements associated with integrating the new capability into the operational environment. This includes integration and interoperability with other IT systems in the BLM.
Human Integration	Define human-product integration requirements to achieve optimum performance from a total product perspective. Define requirements related to employee health and safety. Define requirements associated with special skills and capabilities for operators, maintainers, or support personnel.

Table 15 Requirements Definition Document	
Class of Information	**Description**
IT Security	Define requirements relevant to physical security, contractor-unique security, BLM information security, and security personnel.
Data	Define data requirements addressing how the asset handles data integrity.
Records	Define records requirements describe how records will be maintained.
Architecture	Define architectural requirements and discuss how this new item complies with existing guidance.
CM	Define requirements for the CM of hardware, software, data, interfaces, tools, and documentation.
In-Service Support	Define supportability requirements for the following as appropriate: staffing, supply support, support equipment, technical data, training and training support, first and second level repair, packaging, handling, shipping, and transportation.
Test and Evaluation	Define test and evaluation requirements including scheduled reviews and product assessments. Specify whether independent operational test and evaluation is required. State where operational testing is conducted before testing at an operational site.
Implementation and Transition	Define requirements related to transition from the current capability to the new capability so as to not disrupt on-going BLM operations. Implementation requirements typically encompass implementation planning, preinstallation checkout, installation and checkout, site integration, system shakedown, dual operations, and removal/disposal of replaced systems, equipment, land, facilities, and other items.
Quality Assurance	Define quality assurance requirements for such functions as contractor status reporting, metrics, independent verification and validation, vendor quality assurance, and Capability Maturity Model assessment of the software development processes of potential suppliers.
IMP Select Phase	Define requirements for monitoring, assessing, and optimizing the performance of this capability during acquisition phase of the IMP.

Table 15 Requirements Definition Document	
Class of Information	**Description**
Appendix I. Mission Functionality Matrix	Develop a functionality matrix that maps where every need in the Mission Need Statement is addressed in the RDD.
Appendix II. Definitions	Define non-standard terms used in the RDD.
Appendix III. Acronyms	Define all acronyms used in the RDD.
Attachment - Residual Technical Requirements	Specify those final sponsor requirements that are not intended to be satisfied by the acquisition program approved at the Investment Decision. Resolution of these deferred requirements is the responsibility of the sponsoring program activity.

Chapter 4 Relationships With Other IT Work Activities

4.0 Relationships with other IT Work Activities

This chapter clarifies CM's relationship with other IT work activities. Specifically, CM serves as a bridge to coordinate with IRM's key process areas to ensure that planned and existing IT assets comply with laws and BLM policy, conform to requirements, and that all BLM managed assets are documented, tested, and that information is valid. These activities are universal to the BLM and shall be performed at the National, State, and National Center enterprise-wide level and at the project level.

4.1 Capital Planning, Budget, and IT Investment Management Activities

IT Capital Asset Planning describes the capital planning process for managing IT capital assets, and assists BLM to achieve its performance goals for the use of IT at the lowest possible life cycle cost and the least possible risk. The fundamentals of capital asset planning are outlined in Office of Management and Budget (OMB) Circular No. A-11 (2000). Capital asset planning is a method of ensuring that the needed infrastructure assets (buildings, vehicles, support facilities, equipment) are in place to support an organization.

Over the past years, the Department determined that capital asset planning, budgeting, and acquisition are required for all capital acquisitions with a system life value or total project cost of $2 million or more or that are "highly visible, high risk, or of special importance." In addition, the ITIB may designate any information system project, regardless of cost, as meeting these criteria. Capital asset planning is a prerequisite to obtaining approval of funding for designated IT projects through the budget process.

4.1.1 IT Capital Asset Fund (ITCAF)

The BLM established the ITCAF concept to consolidate IT infrastructure acquisition and maintenance funds in one place. The technology funded from the ITCAF is consistent with the BEA, which defines key business processes and mission requirements. Additionally, it is consistent with the IT architecture as defined in the TRM.

The ITCAF is designed to enable an orderly replacement and predictable maintenance and life cycle based refreshment of BLM's IT. To accomplish this goal without inordinate funding requirements in any single year, funds are allocated, and managed as needed (at both the Washington and the State/National Center levels). The ITCAF provides BLM employees with modern technology on a routine and planned basis as the marketplace evolves.

4.1.2 IT Capital Assets Defined

IT, as defined by the Clinger-Cohen Act of 1996, sections 5002, 5141, and 5142, means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

IT capital assets include the following categories:

1. Data communication equipment, such as Ethernet switches, hubs, routers, and firewalls;

2. Voice communication equipment, such as radio base stations, repeater stations, link radios, microwave equipment, and both analog and digital telephone equipment;

3. Video communication equipment, such as passive satellite, interactive systems, and desktop video systems;

4. Computer equipment, such as desktop and laptop personal computers and applications servers;

5. Major Bureau software, including Bureau systems identified in the corporate baseline by the NCM board. This category includes, but is not limited to, office automation software, electronic messaging systems, network operating and management systems, geographic information systems and software, and database systems;

6. Strategic information systems used to ensure that the public lands and resources are properly managed;

7. Information systems used to provide administrative support to BLM personnel, record financial transactions with the public, and ensure that funds are properly recorded

4.1.3 Distinctions Between the Assets Included in the ITCAF and the BLM Inventory Systems

The ITCAF is designed to ensure that the BLM has the IT assets it needs to sustain and improve productivity. The IT assets described here are different from other capital assets in that normal rules affecting depreciation and replacement do not apply. The IT assets are more susceptible to faster depreciation and replacement. Thus, the Federal property system may include IT assets that have been retired, but not yet surplused; and, IT assets that are purchased for office use, but not defined as part of the BLM corporate baseline. These assets should be incorporated into the Federal property system, but may not be recorded here. The BLM uses as its guide, the expected life of a particular component as indicated by BLM and industry experience.

CM Related Activities

Capital Asset Planning, Budget, and ITIM are business decisions; however, Configuration Managers work with management officials to assure that systems are documented and changes managed.

1. Management officials like CIOs, ITIBs, IRM Chiefs and Program Managers work with Configuration Managers to assure that all IT hardware, commercial software, communication components, and custom-developed software have a planned and funded date when they will be technologically refreshed.

2. Management officials working with Configuration Managers ensure that documents being created to acquire IT assets are placed under formal management.

4.2 Telecommunications Activities

Telecommunications Managers are responsible for providing policy oversight, planning, and operational support to BLM's network infrastructure. This includes radios, routers, telephony equipment, network monitoring devices, firewalls, and associated LAN, and WAN technological devices. Telecommunications Managers, Telecommunications Specialists, and Network Administrators are the core personnel managing the BLM's network infrastructure. They serve as subject matter experts (SMEs) in the area of network load testing, analyzing network traffic, and bandwidth utilization, network protocol analysis, and load balancing technologies and other associated LAN and WAN technologies.

CM Related Activities

Telecommunications Specialists monitor and track the health of BLM's embedded LAN and WAN infrastructure. They are also responsible for ensuring that telecommunications IT assets are documented and configurations validated. It is crucial that application developers and system maintainers consult with telecommunications SMEs in the planning phase of upgrades and newly acquired IT assets.

1. Telecommunications Specialists work with Configuration Managers to baseline all infrastructure hardware and software.

2. Telecommunications Specialists work with Configuration Managers to assure that changes are coordinated and managed according to the established change management process.

3. The Configuration Manager serves as a liaison between project staffs, end-user community, and other IT professionals to ensure that application, system and telecommunications changes are managed, planned, reported, documented, and communicated throughout all levels of the organization.

4.3 BLM BEA Activities

The BEA effort is the primary vehicle used by the BLM to define and analyze its current target business processes (P), data (D), applications (A), and technology (T). The analysis, in turn, leads to recommendations that facilitate improved business-driven land and resource management decisions. The BEA focuses on partnering with business process owners to improve and capture re-engineered processes and supporting data requirements. It also identifies opportunities to minimize redundant, nonstandard data through the establishment of enterprise information data stores. The target technology architecture is documented in the TRM which defines IT standards and products approved for purchase throughout the BLM. Finally, the BEA has established architectural governance policies and boards such as architectural alignment criteria and the TRB to ensure proposed and ongoing projects adhere to the BEA.

CM Related Activities

The National Configuration Manager is a member of the TRB and works with the Board to develop and implement an Enterprise CMP that goes beyond the IRM community. They also work closely together to coordinate updates to the National baselines and the baseline data reflected in the TRM.

The IT Architect works with the National Configuration Manager to ensure the CM baselines are coordinated and the IT Asset history is reflected accurately in the TRM.

1. The Board prepares status reports for the ITIB, CIO, and other affected parties related to Architectural Compliance and Baseline Maintenance.

2. The National Configuration Manager ensures the integrity of the national product baseline.

3. The National Configuration Manager serves as a liaison between project staffs, end-user community, and other IT professionals to ensure that application, system and changes to architectural documents are managed, planned, reported, documented, and communicated throughout all levels of the organization.

4. Configuration Managers ensure that products identified for "Containment" are not being submitted for upgrades, throughout the BLM offices.

4.4. Acquisition and Contracts Activities

Acquisition and Contract staffs serve as SME with Federal Acquisition Regulations (FAR) and provide advisory services on contract vehicles like SLAs, Memorandum of Understandings, Task Orders or Statements of Work., and Performance Based Contracting, Request For Quotes, Small Business, General Services Administration Schedules, and other associated obligation vehicles.

CM Related Activities

1. Configuration Managers ensure that language regarding CM standards are reflected in all software development contracts.

2. Configuration Managers will use SLAs where appropriate to clarify testing support requirements. The SLA will serve as a tool to identify specific processes to be accomplished within set delivery dates. Service levels should be negotiated and agreed to by the parties directly affected. Specific areas that must be included are as follows:

    A. Terms of the agreement and when they take effect and for what period of time

    B. Funding source for the service

    C. Authorizations

D. Deliverables

E. Performance Measures and Outcomes

3. Contract staff coordinate software acquisition activities through the Configuration Manager to assure the IT asset being acquired was coordinated through the CM staff.

4.5 Data Management Activities

The Data Management program is responsible for establishing, maintaining, and preserving the integrity and security of data collected, used, and shared within the BLM. Data Administration includes the concepts of data quality, data privacy, data security, and database integrity. They maintain the Corporate Meta Data Repository.

CM Related Activities

The Bureau Data Administrator is a member of the NCCB.

1. Data Administrators work with Configuration Managers to establish Configuration Item Identifiers for use within the CM tracking number.

2. Data Administrators serve as SMEs to assess the quality of data within CM electronic repositories for compliance to current data standards.

3. Data Administrators review application development projects for compliance to data standards and data quality.

4. Data Administrators serve as certifying officials on projects for compliance to the data program requirements.

4.6 Records Management Activities

The Records Management program is responsible for 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. Records are all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government 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 Government or because of the informational value of the data in them.

CM Related Activities

The Bureau Records Administrator is a member of the NCCB.

1. Records Administrators work with Configuration Managers to establish Subject Codes for CM documentation.

2. Records Administrators work with Configuration Managers to setup Disposition Programs for documentation under CM control.

3. Records Administrators serve as SMEs on all related records issue that affect CM activities.

4. Records Administrators serve as certifying officials on projects for compliance to the records program.

4.7 IT Security Activities

The IT Security program is responsible for establishing policy and procedures for managing all aspects of information security which include administrative, personnel, technical, physical, and telecommunications security. They conduct risk assessments, perform security awareness training , monitor network security, and are authorizing officials for creation and setup of user accounts.

CM Related Activities

The Bureau IT Security Administrator is a member of the NCCB.

1. IT Security Administrators work with Configuration Managers on the CMP for Anti-Virus Defense Software configurations, installations, and distributions.

2. IT Security Administrators serve as SMEs on all related IT security issues that affect CM activities.

3. IT Security Administrators serve as certifying officials on projects for compliance to the IT Security program

4.8 Freedom of Information Act (FOIA) Activities

The FOIA (5.United States Code [U.S.C] 552) program is responsible for safeguarding the confidentiality of sensitive personal, commercial, and other privileged Agency information. The program is also responsible for assuring compliance with federal regulations governing the Privacy Act (5.U.S.C. 552a), and Section 508 of the Rehabilitation Act (29 U.S.C. 794d).

CM Related Activities

The Bureau FOIA/Privacy Officer works with the National Configuration Manager in developing an integrated CM policy.

1. The Bureau FOIA/Privacy Officer works with Configuration Managers on privacy issues with system development activities and existing systems.

2. Privacy Officers serve as SMEs all related privacy issues that affect CM activities.

3. Privacy Officers serve as certifying officials on projects for compliance to the Privacy Program considerations with systems and manual records.

4.9 Life Cycle Management Activities

Life Cycle Management (LCM) is the process of managing a system from cradle to grave. It represents a structured approach to solving information management needs. LCM covers a broad range of activities, from the identification of a problem or need, to the replacement and archiving of the system. The BLM supplemented its application of LCM with the creation of the BLM IMP.

CM Related Activities

1. Configuration Managers coordinate with sponsors, system owners, and project managers to ensure that systems are documented, tested, and validated within the appropriate stage of their life cycle and the correlating IMP stage.

2. Configuration Managers monitor, track, and provide status reports on investments throughout their life cycle.

Glossary of Terms

Acceptance. The act of an authorized representative of the Government by which the Government assumes ownership of supplies as partial or complete performance of the contract. (Excerpt from FAR 46.101)

Application software. Software designed to fulfill specific needs of a user; for example, software for navigation, payroll, or process control. Contrast with: support software; system software.

Approval. Written notification that plans, design, or other aspects of the project appear to be sound and can be used as the basis for further work. Such approval in no way shifts responsibility from the project manager or contractor to meet requirements.

Baseline. A snapshot of an IT assets configuration items from its initial planned version to its approved released version. A specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development or acquisition, and that can be changed only through formal CM process change control procedures. (IEEE-STD610)

Change Notice. A form used by Configuration Managers to track and monitor system changes.

Change Request. A form to submit modifications to documents, applications, and hardware under formal CM.

Charter. A document setting forth the principles, functions, and organization of a corporate body.

Commercial off-the-shelf (COTS). An item produced and placed in stock by a distributor before receiving orders or contracts for its sale. (Excerpt from FAR 46.101)

Computer hardware. Devices capable of accepting and storing computer data, executing a systematic sequence of operations on computer data, or producing control outputs. Such devices can perform substantial interpretation, computation, communication, control, or other logical functions.

Computer resources. The totality of computer hardware, software, personnel, documentation, supplies, and services applied to a given effort.

Computer software (or software). A combination of associated computer instructions and computer data definitions required to enable computer hardware to perform computational or control functions.

Computer Software Configuration Item (CSCI). An aggregation of software that satisfies an end use function and is designated by the Government for separate CM. CSCIs are selected based on tradeoffs among software function, size, host or target computers, developer, support concept, plans for reuse, criticality, interface considerations, need to be separately documented and controlled, and other factors.

Configuration Item. An aggregation of hardware, software, or both that satisfies an end use function and is designated by the Government for separate CM.

Configuration Management. is a disciplined approach to managing Information Technology assets based on industry standards and models. It is one of the key processes the BLM uses to formally manage its IT assets throughout their life cycle.

Contracting agency. As used in this standard, the contracting office as defined in FAR Subpart 2.1, or its designated representative.

Control. CM terminology used to define the management of products under CM such as changes to any project software and/or application that is released into the production environment.

Database. A collection of data, often containing data for more than one application and usually supported by a Database Management System (DBMS). Contrast with data bank.

Document. A data medium and the data recorded on it, that generally has permanence and that can be read by humans or machines.

Evaluation. The process of determining whether an item or activity meets specified criteria.

Fast Track. Fast Track is the process used by BLM to deploy COTS and other priority software products into the environment.

Firmware. The combination of a hardware device and computer instructions or computer data that reside as read only software on the hardware device. The software cannot be readily modified under program control.

Functional Configuration Audit. A review conducted to verify that computer software configuration item complies with unit specification documentation.

Hardware Configuration Item (HWCI). An aggregation of hardware that satisfies an end use function and is designated by the Government for separate CM.

Life cycle management. The process of managing an IT asset from cradle to grave.

Life cycle model. A framework containing the processes, activities, and tasks involved in the development, operation, and support of a system, spanning the life of the system from the definition of its requirements to the termination of its use.

Physical Configuration Audit. A review conducted to verify that system specification documentation correctly and fully describes the computer program product configuration.

Problem Report. An electronic record of problems with hardware and software IT assets that may be used to generate improvements to those assets.

Process. An organized set of activities performed for a given purpose; for example, the software development process.

Review. A process or meeting during which a work product or set of work products is presented to project personnel, managers, users, customers, or other interested parties for comment or approval.

Software development or application development activity. Software and associated data created, modified, or incorporated to satisfy a software development contract. Examples include plans, requirements, design, code, code listings, test information, and manuals.

Software engineering environment. The set of automated tools, firmware devices, and hardware necessary to perform the software engineering effort. The automated tools may include but are not limited to computer-aided software engineering (CASE) tools, compilers, assemblers, linkers, loaders, operating system, debuggers, simulators, emulators, test tools, documentation tools, and database management systems.

Software support. The sum of all activities that take place to ensure that implemented and fielded software continues to fully support the operational mission of the software.

Software test environment. A set of automated tools, firmware devices, and hardware necessary to test software. The automated tools may include but are not limited to test tools such as simulation software, code analyzers, test case generators, path analyzers, etc. and may also include those tools used in the software engineering environment.

Software unit. A logical element in the design of a CSCI; for example, a class, object, module, function, routine, or database. When implemented in code, a logical grouping of computer instructions, data definitions, and/or data.

Support software. Software that aids in the development or maintenance of other software, for example, compilers, loaders, and other utilities. Contrast with application software; system software.

System software. Software designed to facilitate the operation and maintenance of a computer system; for example, operating systems, diagnostic software, and other utilities. Contrast with: application software; support software.

Validation. The process of checking compliance of data with preset standards and verifying data correctness.

Verification. The process of evaluating the products of a given software development activity to determine correctness and consistency with respect to the products and standards provided as input to that activity.

Version. A modification to a software product to correct deficiencies or problems identified in an earlier release

Appendix 1 - Acronyms and Abbreviations

ACM	Acquisition Configuration Management
AD	Assistant Director
AP	Acquisition Plan
BCMT	BLM Configuration Management Team
BEA	Bureau Enterprise Architecture
BLM	Bureau of Land Management
BMP	Baseline Management Process
CASE	Computer-aided Software Engineering
CIO	Chief Information Officer
CM	Configuration Management
CMM	Capability Maturity Model
CMP	Change Management Process
CMR	Corporate Metadata Repository
CN	Change Notice
COTS	Commercial-off-the-Shelf
CSCI	Computer Software Configuration Item
CR	Change Request
DBMS	Database Management System
FAR	Federal Acquisition Regulation
FCA	Functional Configuration Audit
FOIA	Freedom of Information Act
FO	Field Office
GAO	General Accounting Office
GPRA	Government Performance Results Act
HCM	Hardware Configuration Management
HRS	Hardware Requirements Specification
HWCI	Hardware Configuration Item
IEEE	Institute of Electrical and Electronic Engineers
IDD	Interface Design Document
IM	Instruction Memorandum
IMP	Investment Management Process
IP	Implementation Plan
IRM	Information Resource Management
IRS	Interface Requirements Specification
IT	Information Technology
ITA	Information Technology Architecture
ITCAF	Information Technology Capital Asset Fund
ITIB	Information Technology Investment Board
LAN	Local Area Network
LCM	Life Cycle Management
MilStd	Military Standard

MTP	Master Test Plan
NCCB	National Configuration Control Board
NCM	National Configuration Management
NIFC	National Interagency Fire Center
NIRMC	National Information Resource Management Center
NTL	National Test Lab
OMB	Office of Management and Budget
PCA	Physical Configuration Audit
PDF	Portable Document Format
POC	Point of Contact
PR	Problem Report
QPL	Qualified Providers List
RCP	Request for Change Proposal
RDD	Requirements Definition Document
RFP	Request for Proposal
RSL	Requirements Summary List
RTM	Requirements Traceability Matrix
SCM	Software Configuration Management
SCO	System Coordination Office
SDD	System Design Document
SDP	Software Development Plan
SEI	Systems Engineering Institute
SLA	Service Level Agreement
SME	Subject Matter Experts
SOP	Standard Operating Procedure
SPS	Software Product Specification
STD	Software Test Description
STP	Software Test Plan
SRC	Source Code
SRF	Support Request Form
SRS	Software Requirements Specification
TRB	Technical Review Board
TRM	Technical Reference Model
VDD	Version Description Document
WAN	Wide Area Network

Appendix 2 - Best Practices
Based on IEEE Standards
Tailored for BLM's Needs

Software Acquisition

Introduction:

The BLM acquires both COTS products and custom-COTS products. Therefore, it is critical to use best practices to ensure the BLM maximizes its return on investment. COTS software is defined by a market driven need. Because it is commercially available and its fitness for use has been demonstrated by a broad spectrum of commercial, the COTS supplier does not advertise any willingness to modify the software for a specific customer. Meanwhile, custom-COTS products are similar to COTS products; however, custom-COTS products advertise services to tailor the product to the acquirer-specific requirements.

The following best practices are recommended for software acquisitions:

1. Document the process.

A good process should follow the phases software acquisition life cycle. The phases within the life cycle are broadly defined by a set of milestones that establish the beginning and ending of each phase. These phases and their key milestones are as follows:

a. Planning phase. This phase begins when the idea or need is established for acquiring software and ends when the request for proposal (RFP) is released.

b. Contracting phase. After the RFP is released, this phase includes activities necessary to ensure that the supplier's products and services can satisfy the acquirer's quality criteria before signing the contract.

c. Product implementation phase. This phase covers the period from contract signing until the software has been received.

d. Product acceptance phase. This phase includes all activities necessary to evaluate, test, and accept the software product.

e. Follow-on phase. After the software product is accepted, this phase includes using the product to meet the acquirer's objectives and evaluating users satisfaction with the software product, its documentation, and support provided from the supplier.

The following nine steps describe how to build quality into the software acquisition process.

Step 1: Planning organizational strategy. Review acquirer's objective and develop a strategy for acquiring software. *This is required under the Select Phase within the IMP.*

Step 2: Implementing organization's process. Establish a software acquisition process that fits organization's needs for obtaining a quality software product. Include appropriate contracting practices. *Established and working throughout the BLM exclusive of the newly implemented IMP.*

Step 3: Determining the software requirements. Define the software being acquired and prepare quality and maintenance plans for accepting software supplied by the supplier. *The IMP currently requires a Quality Plan within the Select Phase*.

Step 4: Identifying potential suppliers. Select potential candidates who will provide documentation for their software, demonstrate their software, and provide formal proposals. Failure to perform any of these actions is a basis to reject a potential supplier performance data from previous contracts. *Established and working throughout the BLM exclusive of the newly implemented IMP.*

Step 5: Preparing contract requirements. Describe the quality of work to be done in terms of acceptable performance and acceptance criteria, and prepare contract provisions that tie payments to deliverables. *The IMP currently requires an Acquisition Plan within the Select Phase*.

Step 6: Evaluating proposals and selecting the supplier. Evaluate supplier proposals, select a qualified supplier, and negotiate the contract. *Established and working throughout the BLM exclusive of the newly implemented IMP.*

Step 7: Managing supplier performance. Monitor supplier progress to ensure all milestones are met and to approve work segments. Provide all acquirer deliverables to the supplier when required.

Step 8: Accepting the software. Perform adequate testing and establish a process for certifying that all discrepancies have been corrected and that all acceptance criteria have been satisfied. *The IMP currently requires a Design Review, System Acceptance and User Acceptance Plan within the Control Phase. The CM process requires that IT assets are tested, and validated prior to acceptance and deployment.*

Step 9: Using the software. Conduct a follow-up analysis of the software acquisition contract to evaluate contracting practices, record lessons learned, and evaluate user satisfaction with the product. Retain supplier performance data. *Established and working throughout the BLM exclusive of the newly implemented IMP. Re-emphasized within the IMP within the Evaluate Phase.*

2 Publish and communicate the process.

Table 16 describes the current process documented in the IMP.

Table 16 Key Process Steps for Acquisitions at the National Level

IMP Phase	Responsible Party	Steps[a] in Acquisition Process	Inputs to Steps [b]	Outputs from the steps
Select	Planning Phase (Project Manager, SCO) TRB Review for architectural compliance.	1. Planning organizational strategy	· Business Case · Acquirer's objectives · Project Plan	· Quality characteristics of software. · Organizational strategy for acquiring software. · General practices.
		2. Implementing organization's process	· Acquisition Plan · CM Plan · IT Security Plan · Data management Plan	· Establish the SW · Supplier qualification
		3. Determining the software requirements	· Functionality matrix · Quality Plan content ·Supplier evaluation Criteria $ Acquirer and supplier obligations	· SW being acquired · Quality Plan defined. · Proposal evaluation standards. · Contingency Plan
	Contracting Phase · Project	4. Identifying potential suppliers	· Supplier performance $ Supplier evaluation criteria (3) $ Definition of SW $ Results being acquired $ User Survey Questionnaire	$ RFP $ Information of SW $ Qualified Provider's list $ User Survey
		5. Preparing Contract Requirements	$ Supplier and acquirer responsibilities $ Supplier performance standards (7) $ Acquirer's terms and conditions $ Quality Assurance clauses $ Payment Provisions (8)	$ Acceptance Criteria $ Supplier Performance $ Evaluation and test $ Tie payments to $ Prepared contract
		6. Evaluating Proposals and selecting a supplier	$ Supplier proposals $ Proposal evaluation standards $ Quality Assurance clauses $ User Survey Results (6)	$ Evaluation of proposals $ Evaluation of suppliers $ Supplier Selection $ Negotiated Contract

Table 16 Key Process Steps for Acquisitions at the National Level				
IMP Phase	Responsible Party	Steps[a] in Acquisition Process	Inputs to Steps [b]	Outputs from the steps
Control	Product Implementation Phase (Design Development) $ Project Manager, SCO and Contracting Officer $ TRB Review for architectural compliance.	7. Managing supplier performance	• Negotiated contract $ Contract milestones $ Acquirer's deliverables provided to supplier $ Supplier performance criteria $ Monitor supplier progress $ Master Test Plan Content $ System Design Content	$ Work segments approved $ Completed milestones $ Software Deliverables $ Feedback to the supplier $ Master Test Plan $ System Design Document
	Product Acceptance Phase $ Project Manager, SCO and Contracting Officer $ NCCB CM Review and Design modification tracking	8. Accepting the SW	$ Acceptance criteria $ Evaluation criteria $ Test criteria $ Quality Plan $ Supplier performance criteria $ Establish acceptance process (12) $ Design modification tracking	Acceptance process $ Test Descriptions $ Test procedures $ Version Description $ Test Reports $ Support Request Form $ User Guide $ System Design
Evaluate	Follow-on Phase $ Project Manager, SCO and Contracting Officer $ NCCB Review for CM compliance	9. Using the SW	$ Software deliverables $ Documentation $ Support Available $ Quality Plan $ Maintenance Plan	$ Contracting practices evaluated $ User satisfaction assessment $ Supplier performance data

[a]The step numbers correlate to the nine steps identified under Section 1-Document the process.
[b]The numbers in parentheses refer to the checklists listed on the National CM Website. Samples of some checklists are included in Appendix 3.

Success can be achieved in acquiring high quality software products through exercising the nine steps identified within the software.

Appendix 3 - Checklists

C-1 Checklist 1: Organizational strategy.

1. Who will provide software support?	Supplier	Acquirer
2. Is maintenance documentation necessary?	Yes	No
3. Will user training be provided by the supplier?	Yes	No
4. Will acquirer's personnel need training?	Yes	No
5. When software conversion or modification is planned:		
a. Will supplier manuals sufficiently describe the SW?	Yes	No
b. Will specifications be necessary to describe the conversion or modification requirements and the implementation details of the conversion or modification?	Yes	No
c. Who will provide these specifications?	Supplier	Acquirer
d. Has the sponsor approved these specifications?	Yes	No
6. Will source code be provided by the supplier so that modifications can be made?	Yes	No
7. Are supplier publications suitable to end users?	Yes	No
a. Will unique publications be needed?	Yes	No
b. Are there copyright or royalty issues?	Yes	No
8. Will the software be evaluated and certified?	Yes	No
a. Is a survey of the supplier's existing customer sufficient?	Yes	No
b. Are reviews and audits desirable?	Yes	No
c. Where will testing be performed?	NTL	Other
d. Who will perform the testing?_____		
e. When will the software be ready for acceptance? _____		
9. Will the supplier support be needed during initial installations of the software by end users?	Yes	No
10. Will subsequent releases of the software be made?	Yes	No
a. If so, how many? _____Will they be compatible with each other?	Yes	No
11. Will the acquired software require rework whenever operating system changes occur?	Yes	No
12. Will the acquired software commit acquirer's organization to continue some software product, such as a language, that could possibly be discontinued in the future?	Yes	No
13. What are the options/risk if the software is not required?_____		

Approved:

System Sponsor Date Project Manager Date

C-2 Checklist 2: Define the Software

1. Rate the Importance of the following aspects of the software being acquired.
   a. Software specification — Important — Not Important
   b. Functional requirements — Important — Not Important
   c. Any known constraints or parameters — Important — Not Important

2. Rate the importance of the deliverables to be included with the software being defined.
   a. Software description — Important — Not Important
   b. Source code listings — Important — Not Important
   c. Object code listings — Important — Not Important
   d. User manuals — Important — Not Important
   e. Support publications — Important — Not Important
   f. List of current users (existing SW product) — Important — Not Important

3. Rate the importance of the software support to be provided with the software being defined?
   a. User training — Important — Not Important
   b. Internal training — Important — Not Important
   c. Post-installation support — Important — Not Important
   d. Correction of errors — Important — Not Important
   e. Modifications, when requested — Important — Not Important
   f. Software warranty — Important — Not Important
   g. Documentation warranty — Important — Not Important

I certify that I have reviewed the system and documentation in my subject matter area and I have provided comments to the Project Manager.

_____ _____
IT Security Officer Date

_____ _____
IT Records Manager Date

_____ _____
IT Data Manager Date

_____ _____
Configuration Manager Date

Approvals:

_____ _____
System Owner Date

_____ _____
Project Manager Date

C-3 Checklist 3: User survey

Operation

1. Is the system easy to use?	Yes	No
2. What is the level of technical knowledge required to Use and maintain the system?_____		
3. Have there been any serious operator complaints?	Yes	No
4. Was adequate operator and support training given?	Yes	No
5. How long did it take the acquirer's operator to become familiar with the system? _____		

Reliability

1. How long has the system been in use?_____		
2. During this time, how many updates, error corrections, and enhancements have there been? _____		
3. Was the documentation supplied?	Yes	No
4. How many errors have been encountered during this time? _____		
5. What parts of the system are particularly error-prone? _____		
6. What other parts of the system have become unusable And for how long?_____		
7. What errors can be made that will bring the system down?_____		
8. In the event of an error, are there any recovery procedures?	Yes	No
9. How long does it take for a recovery? _____		
10. Is a diagnostic package available on site to verify that The system functions properly?	Yes	No
11. Are supplier backup facilities available?	Yes	No

Maintenance Service

1. How reliable and accessible is the supplier?_____		
2. How frequently is maintenance service required?_____		
3. Are supplier personnel competent in solving problems?	Yes	No
4. What is the average turnaround time between a maintenance service call and the supplier's response?	Yes	No
5. Are backup procedures adequate?	Yes	No
6. How long does backup take?	Yes	No
7. Is there anything error-prone about the procedure?	Yes	No

Performance

1. What are the daily transaction volumes?_____
2. How long does daily processing take? _____
3. What size are the acquirer's files? _____

4. What files are being used? _____
5. How many terminals concurrently process transactions? _____
6. How many users can be on the system before response times becomes sluggish, and how serious is the degradation? _____
7. How have multiple-user degradation problems been solved? _____
8. Is the acquirer's print capacity adequate? Yes No
9. Does the system use spooling for reports? Yes No
10. Are there any terminal lockouts when the printer is running? Yes No
11. What do you envision response time to be? _____

Flexibility

1. What software product modifications have been done?_____
2. Who did the modifications? _____
3. Are changes done on site, where are they done? _____
4. Howe long did changes in each area take? _____
5. What fully developed software has been added? _____
6. Who added the software? _____
7. How long did it take? _____
8. Were there any interface problem? Yes No
9. How has the system been expanded or upgraded?_____
10. How successful was the conversion? _____
11. How much time was involved? _____
12. How much cost was involved? _____
13. How many personnel were involved? _____

Installation

1. Was the system installed as planned? Yes No
2. How long did installation take?_____
3. How much did installation cost? _____
4. Was supplier installation training adequate? Yes No
5. Was supplier installation support competent and complete? Yes No
6. Was the system cut over smoothly? Yes No
7. What anomalies, if any, marred the installation? _____
8. What environmental changes were required to install the system? _____

Costs

1. What unanticipated charges were incurred during installation? _____
2. What unanticipated charges were incurred after installation?

_____

3. Is the acquirer's service agreement cost-effective? Yes No
4. What have new product enhancements from the supplier cost?_____

5. What charges, if any have been incurred to update or correct software?_____
6. Does customized software work also include updated documentation? Yes No
7. What does customized software work cost?_____
8. In what areas have you found the system to be most cost-effective?_____
9. In what areas have you found the system to be least cost-effective?_____

Security

1. Are users and file security levels adequate?	Yes	No
2. Can unauthorized transactions or programs be run?	Yes	No
3. Are accounting audit controls satisfactory?	Yes	No
4. Do accounting audit controls satisfy the acquirer's contracting office?	Yes	No

I certify that I have reviewed the system and documentation in my subject matter area and I have provided comments to the Project Manager.

_____	_____
User Representative	Date
_____	_____
IT Security Officer	Date
_____	_____
IT Records Manager	Date
_____	_____
IT Data Manager	Date
_____	_____
Configuration Manager	Date

Approvals:

_____	_____
System Owner	Date
_____	_____
Project Manager	Date

Appendix 4 - Forms

Form 1268-1 (Rev C)
(March 2003)

United States
Department of the Interior
Bureau of Land Management
Change Request (CR)

1. CR Number:

2. CR Revision:

3. Requestor:	4. Phone Number: ( ) - x	5. Date: [ ] MM/DD/YYYY	6. Office Code:	7. Email Address:	8. Fax Number: ( ) - x
9. Requested Change:					
10. Reason for Change:					
11. Proposed Solution:					
12. What would be the impact if this change is disapproved?					

For CM Use Only

13. Recommendation/Solution:	14. Priority for Review: Priority: Class: Risk:
15. Business Impact:	

Items Affected:

16. Documents: ☐ Yes ☐ Not Applicable	17. Hardware: ☐ Yes ☐ Not Applicable		18. Software: ☐ Yes ☐ Not Applicable		19. Other:

Disposition Authority:

20. Date: [ ] MM/DD/YYYY	21. Title: Signature:	22. Action:
23. Comments:		

Instructions on page 2

Change Request Description

Block 1: ***CR Number.*** Please leave blank, the local Configuration Manager will assign this number.

Block 2: ***CR Revision.*** Please leave blank, the local Configuration Manager will assign this number. This field is completed if there is an existing CR being processed and there is a change needed for that CR.

Block 3: ***Requestor.*** Please enter your name.

Block 4: ***Phone Number.*** Please enter your telephone number.

Block 5: ***Date.*** Please enter the current date.

Block 6: ***Office Code.*** Please enter your office code.

Block 7: ***E-mail address.*** Please enter your electronic mail address.

Block 8: ***Fax number.*** Please enter your fax number.

Block 9: ***Requested Changed.*** Briefly describe the change. For instance, upgrade software, modify document to include installation instructions for new systems, etc.

Block 10: ***Reason for Change.*** Briefly describe the reason for change. For example: Security leak was identified in the existing released version.

Block 11: ***Proposed Solution.*** Briefly describe the proposed solution. For example: Upgrade software to the current release to fix security leaks identified in the previous release.
Block 12: ***What would be the impact if this change is disapproved?*** Briefly describe the impacts to the BLM if the change is disapproved in the terms of cost, information exchange, safety, security, etc.

Block 13: ***Recommendation/Solution.*** This block is for CM Use Only. The local board or Configuration Manager reviews the change request, recommends acceptance of proposed solution or recommends an alternative solution.

Block 14. ***Priority for Revie***w. There are three priority levels for review:
Priority 1 — Urgent determined by impacts to the BLM
Priority 2 — Fast track usually reserved for existing systems
Priority 3 — Standard usually reserved for new systems under ITIB review.

Enter the appropriate priority level. Priority for review is also determined by system and application class, and risk level.

Classes assist Configuration Managers with a quick assessment on the population impacted: Class 1 — BLM National Systems, Class 2 —Departmental Systems, Class 3 — Multi-use State Systems, Class 4 — Statewide systems, Class 5 — Office systems, and Class 6 — Group systems. Enter appropriate class level.

Risk levels are represented by
High Risk — assigned to software and application systems that pose security risks, threaten security of financial data or may compromise the network infrastructure (servers, routers and desktop systems). High risk may cause a rescheduling of other activities.
Medium Risk — assigned to existing software and applications undergoing upgrade, bug fixes.
Low Risk — assigned to new applications and COTS software under the ITIB, because they are undergoing evaluation, and testing and need approval from the ITIB after completion prior to deployment. Enter appropriate risk level.

Block 15: ***Business Impact.*** Configuration Manager must describe business impact based on prescribed information in blocks 9 through 14.

Under Items Affected check all that apply.

Block 16: ***Documents.*** If the change affects documentation, put a check in the box, if it does not then enter not applicable.

Block 17: ***Hardware.*** If the change affects hardware, then put a check in the box, if it does not then enter not applicable

Block 18: ***Software.*** If the change affects software, then put a check in the box, if it does not then enter not applicable.

Block 19: ***Other.*** Configuration Managers should list Configuration Items (CI) that fall outside of documents, hardware, and software.

Block 20: ***Date.*** Enter the date signed by the Configuration Manager.

Block 21: ***Title.*** Enter the name of the Configuration Manager.

Block 22: ***Action.*** Enter approved, approved with stipulations or disapproved. One possible reason for approved with stipulations might be additional information required to meet configuration requirements.

Block 23: ***Comments.*** Enter all comments here like stipulations for the requestor or for review by higher authority to make the decision.

Change Notice

For CM Use Only	
1. Change Request (CR) Numbers: List all CR numbers processed on this form.	*2. Date:*
_____ *3. Completed by:* *CM Representative*	*4. Date:*
5. Documents To Be Created or Changed.	

CI Number	*Old Revision*	*New Revision*	*Task Descriptions*	*Targeted Due Date*	*Completion Date*	*Responsible Parties*
6. Software To Be Developed, Placed Into Service or Changed.						
CI Number	*Old Version #*	*New Version #*	*Task Descriptions*	*Targeted Due Date*	*Completion Date*	*Responsible Parties*
7. Hardware To Be Placed Into Service or Changed.						
CI Number	*Type*	*OS*	*Task Descriptions*	*Targeted Due Date*	*Completion Date*	*Responsible Parties*
8. Comments						

Change Notice Description

Introduction:

The Change Notice (CN) is an internal control record used by the Configuration Manager to track and monitor a Change Request (CR) to furnish and preserve the physical item hierarchy of configuration items, to ensure that all affected configuration items are coordinated and changes implemented within the agreed upon time frames set by the local Configuration Board, Configuration Manager and the responsible parties. It provides an implementation schedule for approved change requests. When completing this form, each line represents a single item except under task descriptions and responsible parties which allow for multiple data entries.

Block 1: ***List all CR numbers processed on this form.*** This form is ideally suited to process and document a single Change Request. A Change Request may be processed on a single form. The Configuration Manager must use care to ensure that when processing multiple Change Requests that sufficient room exists to document all affected configuration items.

Block 2: ***Date.*** List all dates in mm/dd/yyyy format. The date the Change Request was received by the Configuration Manager.

Block 3: ***Completed by.*** Configuration Manager must sign the form when all the information is recorded.

Block 4: ***Configuration Manager.*** Signature of Site Configuration Manager.

Block 5: ***Documents To Be Created or Changed.*** List all documents to be created or changed in this section. Each document like a VDD, Test Report, User Guide, etc., has an associated configuration item identification (CI) number. CI numbers are generated from your local tracking system and are assigned by the Configuration Manager. Please fill in the columns with the appropriate information. Document revision numbers are represented in a numeric format such as 1.0, 1.1, 1.2, etc. If it is a change to an existing document then the new revision number is represented by the next numeric iteration. The first number in the sequence (1.0) represents the document if it is an entirely new document. List all dates in mm/dd/yyyy format. List the targeted due date, the actual completion date and the person responsible for performing the task.

Block 6: ***Software To Be Developed, Placed Into Service or Changed.*** List all affected software with correlating CI numbers. If it is an existing COTS or application, then record the old version number and the new version. These fields are up to seven characters such as V4.79.00a which would stand for Version 4.79a. If it is a new COTS product or application, you will only use the new version number field. Please complete the rest of the fields according to the information requested: task descriptions, targeted due date, completion date and responsible parties.

Block 7: ***Hardware To Be Placed Into Service or Changed.*** List all affected hardware. Record the hardware CI number; it is the configuration item identification number listed for that specific configuration. This could be one CI (configuration) for many physical hardware items. For Type, enter desktop, laptop, server, etc. For OS, list the operating systems affected, W2K, NT, AIX, Sun Solaris, etc. Briefly describe the task associated with implementing the change. Please

complete the rest of the fields according to the information requested: Task Descriptions, Targeted Due Date, Completion Date and Responsible Parties.

Block 8: ***Comments.*** List any comments not covered in the other fields that affect the implementation of change requests being processed and tracked on this change notice. If you are processing multiple change requests, show the linkages between the configuration items. Also discuss any known problems that may have affected the targeted due date.

Support Request Form

Requestor Name:	Requestor Phone Number:
Tester Name:	Tester Phone Number:

Requested Start Date:	Estimated Completion Date:	Estimated Total Number of Hours:

Vendor/Product Information

Vendor Name:	Product Name:
Description of Product:	

Test Specifications

Testing Lab:

☐ National Configuration Test Lab ☐ System Engineering Test Lab

Type of Test:

☐ Performance ☐ Functional/Acceptance ☐ Systems Integration
☐ Interoperability ☐ Regression ☐ Other (e.g., VDD, Installation

Configuration:

	Client Operating Systems		Server Operating Systems
NT Version:		NT Version:	
AIX Version:		AIX Version:	
Win Version:		Lotus Notes Version:	
Other:		Other:	

Communications:

☐ LAN ☐ WAN ☐ 56KB ☐ Non-BLM Site ☐ State T1 Fractional
☐ ATM Backbone ☐ Other

Other Software to be loaded to perform test:

FOR TEST LAB or NCM USE ONLY
Control Number:
NCM #
Assigned Date:
Completion Date:

Special Requirements: (See last page for instructions)

1. Purpose: To determine

2. Strategy: 1.
2.

3. Requirements: 1.
2.

4. Resources:
a. Hardware:
b. Software:
c. Communications:
d. Performance Monitoring Scripts:
e. Personnel and Other Required Assistance:

5. Data Recording, Reduction, and Analysis:

6. Test Procedures:

The special requirements instructions should include all pertinent details regarding the testing such as the following:

1. Purpose (describe the overall purpose of the test)

2. Strategy (describe the testing strategy to be used to perform the test)

3. Requirements (list the requirements which the test is to verify)

4. Resources (describe all resources needed to perform the test)
a. Hardware Resources (IBM J50, F50, 250, Servers, Workstations, PCs (Gateway, Dell, etc.)
b. Software Resources (specify the Operating System with version number and the names of all other software packages to be used along with their version numbers)
c. Communications (LAN, WAN, Inter/intra Site, Non-BLM Site, etc.)
d. Performance Monitoring Scripts (describe the type of monitoring to be performed.
e. Test Personnel and Other Required Assistance (list all personnel who may be involved in the testing)

5. Data Recording, Reduction, and Analysis
a. Describe the type of Data Recording to be used if any
b. Describe Data Reduction process
c. Describe the type of Data Analysis to be done
d. Describe how the Reporting of Results is to be done

5.Test Procedures (describe where the test procedures can be located and they should be available upon request)

FOR TEST LAB or NCM USE ONLY
Control Number:
NCM #
Assigned Date:
Completion Date:

Appendix 5 – Sample Plan

CONFIGURATION MANAGEMENT PLAN

FOR THE

(Insert System Name)

PREPARED FOR:
Bureau of Land Management
(BLM)

PREPARED BY:
Project Manager
Site Location

Approved By:

_____	_____
Project Sponsor	Date
_____	_____
Project Manager	Date
_____	_____
Configuration Manager	Date

Table of Contents

1. Introduction

This plan describes the operating procedures for managing the configurations for the software products identified within the BLM=s Configuration Management (CM) Tools Assessment project. The CM Tools assessment project is designed to look at all existing CM tools within the BLM with the intention of leveraging existing tools to create a comprehensive CM tool kit for project managers, configuration managers and other managerial personnel to effectively conduct CM related activities.

1.1 Purpose

This plan supports the Investment Management Process and is in compliance with the BLMs CM policy.

1.2 Scope

This plan defines the configuration management activities necessary for maintaining all support software items being procured, tested, sustained and kept in the testing and production environment. The list of the software configuration items will vary over time. The consolidated list of configuration items and their status is maintained by the project manager and are available for review by the Technical Review Board, the National Configuration Control Board, Quality Assurance and other concerned parties at the completion of each project milestone.

1.3 Key Terms

List all key terms that apply. *The following list represents possible key terms that you might use.*

CB	Configuration Board
CM	Configuration Management
CMP	Change Management Process
CN	Change Notice
CR	Change Request
HRS	Hardware Requirements Specification
RDD	Requirements Definition Document
RSL	Requirements Summary List
RTM	Requirements Traceability Matrix
SDD	System Design Document
SRS	Software Requirements Specification
SPS	Software Product Specification

STD Software Test Description
STP Software Test Plan
VDD Version Description Document

1.4 Definitions

The terms used in this plan conform to the definitions found in Institute of Electrical and Electronic Engineers (IEEE) Standard Glossary of Software Engineering Terminology.

1.5 References

1. IEEE Std 828-1998, Standard for Software Configuration Management Plans

2. ANSI/IEEE Std 729-1983, IEEE Standard Glossary of Software Engineering

3. BLM Configuration Manual and Handbook

4. BLM's Investment Management Process, Document 1.0

5. Technical Reference Model - Volume II

2. Management

2.1 Roles and Responsibilities

This section describes the roles and responsibilities of the project sponsor and the system owner.

2.1.1 Project Sponsor

The project sponsor is responsible for assigning the project manager. The project sponsor has the approval authority at each CM milestone.

2.1.2 Project Manager

The project manager has oversight and managerial authority over all integrated teams working on CM related activities. The project manager will coordinate their CM project level activities with National Configuration Management staff and complete all CM documentation required to add the products to the National CM baselines.

2.2 Lines of Authority

The following depicts the chain of custody for managing and oversight of the CM Tools project.

National ITIB

Technical Review Board

Reports to the ITIB on architectural compliance issues.

System Coordination Office

Oversight of the project, working with the ITIB to provide guidance and coordinates milestone reviews. Reports to the ITIB

National Configuration Control Board

Oversees final release. Reports findings to the CIO and the TRB.

Project Sponsor

Accountable manager and responsible for the ultimate success of the project. Reports to Project Sponsor line management. May be on the ITIB.

Project Manager

Oversees the work of their Project Configuration Control Board and the Integrated Project Team. Reports to the Project Sponsor and the ITIB through the SCO.

Configuration Control Board

Performs configuration management activities for the project. Reports to the Project Manager.

Integrated Project Team

Members from the business side and technical representatives. Reports to the Project Manager.

3.0 Configuration Management Activities

3.1 Configuration Control

The Project Configuration Control Board is responsible for supporting the change management process for all the support software products in compliance with the CM Manual and Handbook including the Change Request and Change Notice forms. Also, the board is responsible for ensuring that the project uses the correct templates for documenting, tracking, recording, and reporting changes.

3.2 Status Accounting

The Configuration Management Specialist assigned to the project maintains the database used to prepare reports on the status of all support software products and hardware configurations used in the CM Tools project.

3.3 Configuration Identification

The Project Configuration Control Board is responsible for maintaining the identification (numbering, labeling, and integrity of the documentation) for all the support software in the CM Tools project. This extends to identifying the configuration items that are acquired from commercial vendors.

3.3.1 Baseline Identification

Support software product baselines are established upon receipt of the software. Changes and additions to the product baselines will be tested, documented and validated. The Project final product baseline will be released to the National Configuration Management function for integration and performance testing against the existing National CM product and application baselines.

3.3.2 Labeling the Baselines

Labeling the baselines will be in accordance with existing CM policy: As-Planned and As-Released COTS baseline or the As-Planned and As-Release Application baseline.

3.4 Naming and Numbering Conventions

The Configuration Control Board elects to use the existing naming and numbering convention noted in the CM Manual and Handbook.

3.5 Status Reporting

The Project Configuration Control Board will produce a status report for the Project Manager at each identified milestone. The Project manager will forward that report to the Project Sponsor, System Coordination Office, Technical Review Board and the National Configuration Control Board.

3.6 Configuration Audits

The Project manager will conduct an internal configuration audits at each milestone review. Other reviews may be conducted at the request of the Technical Review Board or Project Sponsor.

4. Implementation Schedules

4.1 Project Management Schedule for Pre-Release

The Project Manager will provide the National Configuration Control Board with their pre-release schedules at least one month in advance to enter into discussions regarding the availability of testing facilities to keep project, on schedule and within budget. And, to afford enough time to review proposed documentation needed to release the product to the National CM baseline.

4.2 Project Management Schedule for Post-Release

The Project Manager will provide the National Configuration Control Board with their post-release schedules to begin testing. Project Manager will allocate two weeks time for pre-test to review documentation and setup the test environment. Project Manager will release results of reviews and certifications with the correlating test descriptions, test cases, test plan, change request, support request form to the National Configuration Management electronic mail box ncm@blm.gov.

5. Configuration Management Resources

5.1 Project Team Members

The following table lists the project team members.

Name	**Grade/Step**
Jim Duval Project Manager	GS-XX- Configuration Management Specialist (CO)
Carlton Walker	GS-XX – National Configuration Administrator
Sherman Gillespie	GS-XX – Configuration Management Specialist (WO)
Ralph Bunn	GS-XX – Configuration Management Specialist (CA)
Jim Blancett	GS-XX – Configuration Management Specialist (NIRMC)
David Cavallier	GS-XX – IT Security Manager (NIRMC)
TBD	GS-XX - Data Administrator
Melissa McNichols	GS-XX – System Coordination Office Point of contact
Meleanne Powell	GS-XX Records Administrator
TBD	GS-XX – BLM User Representative
TBD	GS-XX – Network Administrator
TBD	GS-XX – System Administrator
TBD	GS-XX – System Engineer

5.2 Configuration Control Board

The Configuration Control Board will consist of the Records Administrator, IT Security, Data Administrator, Configuration Management Specialist, and a User Representative within the Integrated Project Team.

5.3 Configuration Management Tools

The team will manually process all forms until an automated system is in place. The team will establish an Excel spreadsheet to assign configuration numbers and produce status reports. The team will also use Microsoft Project 2000 to monitor, maintain, and track schedules.

5.4 Facilities

The CM tools will be tested within the National Test Lab at the National Information Resources Management Center within the Systems Engineering Test Environment. The Sponsor will also upon successful testing, pilot the tools for a 30 day period in Denver, Washington, or Oregon.

5.5 Funding

The project will cover all travel required and any additional cost incurred to set up and test the products at the pilot sites.

6. Plan Maintenance

6.1 Access Control

The Configuration Management Specialist assigned to the project who maintains the database will manage and track changes to the plan. All changes will be approved by the Project Manager, System Sponsor, and the Configuration Management Specialist.

6.2 Records Management

All CM records including this plan will be retained and disposed of according to existing Records Management policy.

Appendix 6 – References

1. Bureau of Land Management Annual Performance Plan for Fiscal Year 2002
2. Information Resources Management, Strategic Plan 1997-2002
3. IEEE Std 828-1998, Standard for Software Configuration Management Plans
4. Institute of Configuration Management II
5. General Accounting Office ITIM Process
6. Technical Reference Manual – Volume II
7. USCG – Software Development and Documentation Standards
8. Office of Management and Budget Circulars A-130, A-11
9. IT Security Program Handbook
10. Software Engineering Institute's Capability Maturity Model