Form 1221-2
(June 1969)

UNITED STATES
DEPARTMENT OF THE INTERIOR

BUREAU OF LAND MANAGEMENT

MANUAL TRANSMITTAL SHEET

Release
1-1741

Date
06/19/2012

Subject:
1268-1 Information Technology Configuration Management Manual

1. Explanation of Material Transmitted: This handbook implements the Configuration Management (CM) Manual – MS1268. CM is planning and managing the capacity and resources required to package, build, test, and deploy a release into production and establish the service specified in the customer and stakeholder requirements. CM aims to establish and maintain the integrity of all service assets and configurations, and provide efficient repeatable build and installation mechanisms that can be used to deploy changes to the test and production environments—and be rebuilt, if required to restore service.

2. Reports Required: None.

3. Material Superseded: .

4. Filing Instructions: N/A.

REMOVE:	INSERT:
1268 Release 1-1679	1268
(Total: 12 sheets)	(Total: 13 sheets)

/s/ Lisa L. Jollay
Acting Assistant Director, Information Resources Management
Bureau of Land Management

Information Technology
Configuration Management Manual

BLM Manual 1268

Table of Contents

Chapter 1. Overview

1.1 Purpose

This manual establishes policy, assigns responsibilities, and addresses high-level standards and procedures regarding the Bureau of Land Management (BLM) Information Technology (IT) Configuration Management (CM) Program. CM, as an activity, is the identification, control, recording, reporting, and auditing of IT resources, including their versions, baselines, constituent components, attributes, and relationships. This manual generally covers the four major process groups under the Information Technology Infrastructure Library® (ITIL) Service Transition. Those process groups are: Service Asset and Configuration Management, Change Management, Release and Deployment Management, and Knowledge Management.

1.2 Objectives

This manual establishes and describes the CM program and its interrelationships to other activities. This manual also describes the role of CM in managing existing and future IT assets, and provides management officials and employees with a disciplined approach to documenting, managing, and tracking IT assets throughout their lifecycle.

1.3 Authority

Federal Information Security Management Act of 2002, 44 U.S.C. § 3541. Office of Management and Budget (OMB) Circular No. A-130: *Management of Federal Information Resources* (Revised, Transmittal Memorandum No. 4). *National Institutes of Standards and Technology (NIST) Special Publication 800-53*, Rev 3 (Aug. 2009). The BLM CM process complies with the *Clinger-Cohen Act* "Section 5125 Agency Chief Information Officers, General Responsibilities," the Office of Management and Budget (OMB) Circular A-130 Appendix IV-Analysis of Key Sections, "2. Background," the Capital Planning and Investment Control (CPIC) per the System Development Life Cycle (SDLC) process.

1.4 Responsibility

All personnel responsible for or associated with the use, acquisition, development, and maintenance of BLM's IT resources are also responsible for the CM policy specified in this manual and the associated handbook. The specific responsibilities assigned for CM are as follows:

A. **The Assistant Director-Information Resources Management** (AD-IRM) is responsible for the overall management of BLM IT resources. The AD-IRM also oversees BLM compliance with Federal and Departmental policies, guidelines, and regulations governing the management of IT resources.

B. **The National CM Policy Manager** is responsible for developing and communicating CM policy and ensuring it complies with Federal law, OMB requirements, and Departmental policy and guidance.

C. **The National Operations Center (NOC)** is responsible for the development, testing, deployment, and availability of national IT resources.

D. **The National CM Operations Manager at the NOC** is responsible for coordinating CM activities for the BLM including:

1. Overseeing operation of the National Change Management (NCM) process;

2. Developing procedures to implement an integrated BLM CM program;

3. Overseeing the baselines for national level applications, software, and hardware assets; and

4. Establishing test and implementation priorities for national applications and Commercial-Off-The-Shelf (COTS) products.

E. **Bureau Assistant Directors** (AD) are responsible for ensuring that CM program objectives are carried out within their areas of responsibility and ensuring that skilled staff are assigned to oversee and manage IT resources under their jurisdiction.

F. **State and Center Directors** are responsible for ensuring that CM program objectives are carried out within their areas of responsibility and ensuring that a qualified CM Manager is assigned for their organization.

G. **State/Center IT Managers** are responsible for ensuring that CM program objectives are carried out within their areas of responsibility.

H. **State/Center CM Managers** are responsible for ensuring compliance with this manual and the CM Handbook and:

1. Overseeing State/Center CM activities; and,

2. Providing guidance to State/Center Management and technical personnel on CM policy and procedures.

1.5 References

ITIL, Version 3.0, Office of Government Commerce, United Kingdom.

1.6 Policy

It is the policy of the BLM to manage IT resources as strategic assets—enhancing organizational capabilities and delivering world-class service management for mission-focused activities. It is critical for effective management of IT resources that proper controls are in place to manage configurations and modifications to those resources.

A. **Core Policy Statements (as adopted by ITIL)**.

a. Common Framework. CM activities must use a common framework of standard, re-usable processes and systems to improve integration of the components involved and reduce variations in a process. All processes must be aligned with other BLM processes or related systems to improve efficiency and effectiveness. Where new processes are required, they must be developed for reusability. The CM Handbook details the framework and underlying procedures, processes, standards, and guidelines that must be used bureau-wide for CM program activities.

b. Asset and Configuration Management. IT resources must be identified and tracked in the designated, centralized Configuration/Change Management System (CMS) and underlying Configuration Management Database (CMDB) to the maximum extent practicable as determined jointly by the National CM Policy Manager and National CM Operations Manager.

i. Baseline Configurations. Baseline configurations must be maintained for IT resources. The baseline configuration must be maintained under configuration control within the CMS/CMDB, using automated mechanisms, to the maximum extent practicable. The baseline configurations must be reviewed for validation and verification, and modified as necessary, no less than annually or when significant changes to the IT resources occur, by the responsible systems' authority.

c. Change Management. All changes to IT resources must be implemented through authorized processes associated with the level of change—based on scope and impact, and the types and criticality (priority) of the IT resources.

i. A centralized process for subjected changes to production IT resources must be used in order to minimize the probability of conflicting changes and potential disruption to the production environment.

ii. Only duly authorized officials must be allowed—complying with all relevant policies set forth herein and with all related procedures, standards, and guidelines outlined in the CM Handbook—to make

defined changes to IT resources in the production environment. All others must be denied access to effect said changes.

iii. Changes to IT resources will be defined and governed by a Request for Change (RFC) brought forward in the CM process to ensure effective control and traceability.

iv. Standardized methods and procedures must be used for efficient and prompt handling of defined changes in order to minimize the impact of change-related incidents on business continuity, service quality, and rework.

v. All defined changes and updates to IT resources must be recorded in the proper IT resource (asset) record of the designated CMS and underlying CMDB.

vi. One centralized national CMS and CMDB must be used for all defined changes bureau-wide, as available and designated.

vii. Changes must be properly justified through the development of a clear business case.

viii. Late requests for changes that cannot be properly managed must be remanded for future consideration.

d. Releases and Deployments. Release packages must be planned and designed to be built, tested, delivered, distributed, and deployed into the live environment in a manner that provides the agreed levels of traceability, in a cost-effective and efficient way.

i. All updates to releases must be recorded in the CMS/CMDB.

ii. The CM Handbook must detail release and deployment procedures, processes, standards, and guidelines.

e. National Change Advisory Board (NCAB). An NCAB must operate to execute CM activities effectively and efficiently. The NCAB must be co-chaired by the National CM Policy Manager and the NOC CM Operations Manager. The NCAB must have adequate business and mission representation along with technical, IT security, and operations staff. The meeting will be facilitated and coordinated by alternating CM team members across the BLM.

i. The NCAB will meet on a weekly basis, or as necessary, to discuss and decide on proposed RFCs.

ii. The NCAB must also conduct a separate meeting each month to discuss overall CM program and policy initiatives.

iii. An Emergency Change Advisory Board (ECAB) must be established to address those urgent RFCs where waiting for the routine NCAB meeting is not acceptable. The ECAB may be a subcomponent of the NCAB and related processes and procedures may be utilized.

iv. The CM Handbook must detail the processes to be used by the NCAB and ECAB.

f. Annual Review. This manual and underlying handbook must be reviewed annually, and modified as necessary, to ensure continuing validity, effectiveness, and efficiency of the CM program and related operations throughout the BLM.

B. **Scope**. The policy contained in this document applies to all BLM IT resources, at all levels. This policy is mandatory for all organizational units, employees, contractors, and others having access to, or using, the IT resources of the BLM. This manual applies to all existing and future IT investments. It also applies to all internal service level agreements (SLA) between organizational units, interagency agreements, and contracts made between the BLM and other public and private organizations.

C. **Background**. The Washington Office (WO) and NOC are working together to bring IT CM to a higher level of value for the BLM.

Configuration Management is the maintenance of information about IT assets and their relationships to other assets and business processes. The CM activity also encompasses Asset Management, and Change Management.

Since April 3, 2003, the BLM CM activities have been guided by the Information Technology Configuration Management Manual and Handbook (1268). One major industry advancement and one organizational change prompted modifications to the BLM CM activities and their related manual and handbook. The major industry advancement is due to the availability of a tested framework and approach for IT Service Management, named the ITIL. ITIL seeks to deliver maximum service value through organized processes that support the functions of delivering IT services to customers. It was created by the United Kingdom's Office of Government Commerce.

The organizational change is the result of the Management for Excellence (M4E) initiative in which the NOC was directed to assume operational responsibilities for IT

operations and the WO Information Resources Management Directorate was directed to focus on IT policy and governance.

This activity is expected to streamline the change request process by automating forms and providing access to a comprehensive national CM database, thereby improving service delivery by maintaining real-time configuration information and minimizing IT outages caused by inoperability amongst IT assets and uncoordinated changes.

1.7 File and Records Maintenance

Configuration Management records must be maintained in accordance with BLM records management policy and procedures.

1.8 Coordination Requirements

Configuration Management policy and procedures will be coordinated and disseminated through State and Center configuration managers. These configuration managers will ensure that IT managers; IT security, records, data, and system administrators; help desk personnel; project managers; and, user representatives are kept informed of CM-related activities and that appropriate personnel are included in reviews. State and Center configuration managers will produce status reports of CM activities to share with other configuration managers in regularly scheduled meetings. Project managers will coordinate CM documents, software requests, and testing through the appropriate CM manager.

1.9 Relationships with Other IT Activities

This section describes the roles of other activities that interface with particular aspects of CM. Those activities are as follows:

A. **Data Administration** objectives establish policy, procedures, and standards that guide the BLM's efforts in effective management of information. The focus is on 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.

B. **Freedom of Information Act** (FOIA) objectives provide any person the right to access Federal records, except for records (or portions thereof) that are protected from disclosure by one of nine exemptions. This statute also requires specific information, such as agency rules, regulations, and final decisions are made available as public records. The FOIA is a disclosure statute, but recognizes that the Government is responsible for safeguarding the confidentiality of sensitive personal, commercial, and governmental (proprietary/confidential) information.

C. **IT Security** is responsible for the confidentiality, integrity, and availability of BLM information. The IT Security program includes managing all aspects of information security including administrative, technical, and physical controls.

D. **Life Cycle Management** (LCM) provides a uniform methodology to developing applications and implementing an IT system. LCM is the process of managing a system from concept to retirement. 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.

E. **BLM Telecommunications** provides for the management (planning, operation, and maintenance) of the BLM's telecommunication systems, networks, equipment and services, and define responsibilities. The program provides all BLM telecommunications support in accordance with current statutes, standards, rules, and regulations governing the planning, acquisition, operation, maintenance, and disposal of such capabilities.

F. **Records Administration** objectives establish policy, procedures, and standards for records maintained in electronic and physical form. This includes creation, maintenance, use, disclosure, and disposition of information. Proper administration of records/data/information must be exercised to ensure that the legality, integrity, access, sharing and exchange, and security standards are met. This also includes managing the inventory and disposition of electronic and physical records.

G. Bureau Enterprise Architecture objectives provide a management framework describing "what" needs to happen rather than "how" it should happen. It applies business rules and processes required to operate the organization that are independent of any specific organizational structure, technology, existing systems, hardware, and software needed in basic operation of the BLM.

Glossary of Terms

Asset. An IT resource. *See "Information Technology (IT) Resources".*

Asset Management. The process responsible for tracking and reporting the value and ownership of assets throughout their lifecycle.

Baseline. A Benchmark used as a reference point. A Configuration Management Baseline can be used to enable an IT Resource to be restored to a known Configuration if a Change or Release fails.

Benchmark. The recorded state of something at a specific point in time. A Benchmark can be created for a Configuration, a Process, or any other set of data.

Change. The addition, modification or removal of and IT Resource, or anything that could have an effect on an IT Resource.

Change Management. The process responsible for controlling the lifecycle of all changes. The primary objective of Change Management is to enable beneficial changes to be made, with minimal disruption to, IT Services.

Change Management Database. A database used to store Configuration Records throughout their Lifecycle. The Configuration/Change Management System maintains one or more CMDBs, and each CMDB stores attributes of Configuration Items (CI), and relationships with other CIs.

Configuration. A generic term, used to describe information about IT assets and their relationships and settings.

Configuration Item. Refers to the fundamental structural unit of a configuration management system, the lowest level element to which the organization will manage. The entity must be uniquely identified so that it can be distinguished from all other configuration items.

Configuration Management. The maintenance of information about IT assets and their relationships to other assets and business processes.

Configuration/Change Management System. A set of tools and databases that are used to manage an IT Service Provider's Configuration data. The CMS also includes information about Incidents, Problems, Known Errors, Changes and Releases and may contain data about employees, Suppliers, locations, Business Units, Customers and Users. The CMS includes tools for collecting, storing, managing, updating, and presenting data about all Configuration Items and their Relationships. The CMS is maintained by Configuration Management and is used by all IT Service Management Processes.

Configuration Record. A record containing the details of a CI (IT Resource). Each Configuration record documents the lifecycle of a single CI. Configuration records are stored in a Configuration/Change Management Database.

Deployment. All of the activities necessary to make a software or hardware system available for use.

Information Technology (IT) Resources. IT resources are tools that allow access to electronic technological devices, or are electronic technological devices themselves that service information, access information or is the information itself stored electronically. These resources include all government-supplied computers and servers; desktop workstations, laptop computers, handheld computing and tracking devices; cellular and office phones; network devices such as data, voice and wireless networks, routers, switches, hubs; peripheral devices such as printers, scanners and cameras; pagers, radios, voice messaging, computer generated facsimile transmissions, copy machines, electronic communication including e-mail and archived messages; electronic and removable media including CD-ROMs, tape, floppy and hard disks; external network access, such as the Internet; software, including packaged and internally developed systems and applications; and all information and data stored on BLM equipment as well as any other equipment or communications that are considered IT resources by BLM.

Lifecycle. The various stages in the life of an IT Service, Asset, Configuration Item, Incident, Problem, or Change, etc. The lifecycle defines the categories for status and the status transitions that are permitted.

Policy. A principle or rule to guide decisions and achieve rational outcomes. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of processes, procedures, and standards.

Procedure. A set of actions or operations which have to be executed in the same manner in order to always obtain the same result under the same circumstances. Procedures are defined as part of processes.

Process. A structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs. A process may include any of the roles, responsibilities, tools and management controls required to reliably deliver the outputs. A process may define policies, standards, guidelines, activities, and work instructions if they are needed.

Program. A number of projects and activities planned and managed together to achieve an overall set of related objectives and other outcomes.

Release. A distribution of a collection of hardware, software, documentation, processes or other components required to implement one or more approved changes to IT resources. The contents of each release are managed, tested, and deployed as a single entity.

Release and Deployment Management. Plan, schedule and control the movement of releases to test and live environments. The primary goal of Release Management and Deployment Management is to ensure that the integrity of the live environment is protected and that the correct components are released.

Release Management. Release Management is the central responsible body for the implementation of Changes to the IT Infrastructure, so that these are carried out in an effective, secure and verifiable manner. Their tasks include planning, monitoring and implementation of respective Rollouts or Rollins in coordination with Change Management.

Request for Change. A formal request for a change to be made. A (Request for Change) RFC includes details of the proposed change and may be recorded on paper or electronically. The term RFC is often misused to mean a change record, or the change itself.

Release Packages. A collection of hardware, software, documentation, processes or other components required to implement one or more approved changes to IT services. The contents of each release are managed, tested, and deployed as a single entity.

Appendix – Acronyms and Abbreviations

AD-IRM	Assistant Director – Information Resources Management
BLM	Bureau of Land Management
CD-ROM	Compact Disk – Read Only Memory
CM	Configuration Management
CMS	Configuration/Change Management System
CMDB	Configuration Management Database
CPIC	Capital Planning and Investment Control
ECAB	Emergency Change Advisory Board
FOIA	Freedom of Information Act
FY	Fiscal Year
IT	Information Technology
ITIL®	Information Technology Infrastructure Library®
LCM	Life Cycle Management
M4E	Management for Excellence
NIST	National Institute of Standards and Technology
NCAB	National Change Advisory Board
NCM	National Configuration Management
NOC	National Operations Center
OMB	Office of Management and Budget
RFC	Request for Change
SDLC	System or Software Development Lifecycle
WO	Washington Office