Chief Information Officer
Office of Information Services
Centers for Medicare & Medicaid Services

CMS Policy for
Configuration Management

August 2005

Document Number: CMS-CIO-POL-MGT01-01

TABLE OF CONTENTS

1. PURPOSE

This document establishes the policy for Configuration Management (CM) of Information Technology (IT) assets at the Centers for Medicare & Medicaid Services (CMS) to include all automated systems, software applications and products, supporting hardware and software infrastructure (e.g., equipment, networks, and operating systems), and associated documentation.

2. BACKGROUND

CMS recognizes the necessity of managing its inventory of IT assets and changes to them in a disciplined manner to ensure the integrity and availability of these assets to support CMS' mission. This follows the best practices used by both industry and government. In addition, in its *HHS IRM Guidelines for Capital Planning and Investment Control* (January 2001), the Department of Health and Human Services (DHHS) urged its operating divisions "To fully implement the Clinger-Cohen Act, … to strive, at a minimum, to meet the Software Engineering Institute (SEI) Capability Maturity Model (CMM) level 2, the repeatable level". A successful program of software configuration management is one of the six "key process areas" for achieving "level 2" maturity.

In July 2000, CMS adopted the Institute of Electrical and Electronics Engineers (IEEE) / Electronic Industries Association (EIA) 12207 as the standard to be followed for the CMS System Development Life Cycle (SDLC), in the context of the IEEE's four-volume set, *Software Engineering, 1999 Edition.* The IEEE/EIA 12207 establishes a framework for the life cycle of software and requires configuration management as a "supporting process."

CMS has tailored or customized the IEEE/EIA 12207 standard to meet the specific needs of the Agency, which is documented in the CMS Integrated IT Investment & System Life Cycle Framework. This IT Framework provides a foundation and supporting structure designed to aid in the successful planning, engineering, implementation, maintenance, management, and governance of CMS IT investments and system life cycle projects. Policies, processes, procedures, artifacts, reviews, and standards associated with configuration management are inherent in the CMS IT Framework.

CM is a discipline to ensure that the configuration of an item (and its components) is known and documented, and that changes to it are controlled and tracked. CM applies technical and administrative direction and surveillance over the life cycle of a configuration item (CI) through four basic tenets:

(1) Configuration Identification;
(2) Configuration Control / Change Management;
(3) Configuration Status Accounting; and
(4) Configuration Audits.

3. SCOPE

This policy applies to all IT activities and IT assets owned or controlled by CMS, including those of CMS' agents, contractors or other business partners when acquired or supported by CMS funding. As such, this policy applies to all hardware, software, documentation, and services regardless of origin, nature, or location (e.g., contractor, in-house, development, operations, all hosting data centers, internal and external systems) unless otherwise specified.

4. OPERATIONAL POLICY

The CMS Configuration Management Program consists of a multi-layered structure comprised of policy, processes, procedures and standards, with each layer providing an increasing level of detail. The CM policy, processes, procedures and standards shall be followed unless specifically designated as optional or discretionary.

4.A. CM Planning & Management

All tasks necessary to implement CM principles and to conduct configuration activities shall be planned, coordinated, and managed throughout all lifecycle phases of a project, product, or automated system. The CM planning process shall be fully documented, and the documentation readily available to all levels of development, implementation, and operations management to formalize involvement and ensure continuity of CM practices.

4.B. Configuration Identification

Configuration identification is the process of identifying and documenting the functional and physical characteristics of items that are to be placed under configuration control. Configuration identification includes the selection of CIs, determination of the types of configuration documentation required for each CI, the assignment of unique identifiers to each CI and the technical documentation describing its configuration, and the establishment of configuration baselines. A hierarchical structure shall be established that identifies and summarizes the CIs comprising a given project, product, or automated system. Configuration identification information shall be maintained and readily available to all CMS decision makers.

4.C. Configuration Control / Change Management

Configuration control consists of the evaluation, coordination, approval or disapproval, and implementation of changes to CIs after formal establishment of their configuration identification. Effective configuration control depends on placing products under control at the right time and on establishing mechanisms for controlling changes to the products.

A systematic and measurable change process and procedures shall be implemented that is consistent with industry best practices and CMS' CM policy and standards. The implemented change process and procedures shall ensure proposed changes are properly identified, prioritized,

documented, coordinated, evaluated, and adjudicated. Approved changes shall be properly documented, implemented, verified and tracked to ensure incorporation in all applicable systems and/or products. Changes identified during ongoing maintenance of products/systems operating in production shall cycle forward into new business needs for appropriate analysis and consideration prior to modification of existing, or development of new, products/systems in response to requested changes.

Utilization of a Configuration (or Change) Control Board (CCB) is the CMS-preferred change control forum for establishing CM baselines and approving/disapproving subsequent changes to those baselines. A CCB may exist at the enterprise and/or project level, with an approved charter and operating procedures, as appropriate.

4.D. Configuration Status Accounting

Configuration status accounting focuses on recording and reporting information needed to maintain integrity and traceability of a controlled CI and its associated documentation throughout its life cycle. This includes monitoring the status of proposed changes and the implementation status of approved changes. Status accounting information includes developing and maintaining site configuration data and the incorporation of modification data on products and CIs.

Configuration status accounting information shall be developed and maintained for CIs in a systematic and disciplined manner in accordance with this policy and CMS' CM standards, processes and procedures. This configuration information must be available for use by CMS decision makers over the life cycle of a project, product, or automated system and its identified CIs.

4.E. Configuration Audits

Configuration audits shall be performed to verify that a product's requirements have been met and that the product design meeting those requirements has been accurately documented before a product configuration is baselined or is migrated to the production environment. In addition, developmental and operational systems shall be periodically reconciled against their documentation to ensure consistency between a product and its current baseline documentation. Verification of the incorporation of modifications is a critical function of this activity. Periodic audits of software and hardware configuration baselines in the production environment shall be performed to ascertain that no unauthorized changes have been made without proper approval.

5. ROLES AND RESPONSIBILITIES

The following entities have responsibilities related to the implementation of this policy:

5.A. Chief Information Officer (CIO)

The CIO is responsible for the following activities:

- Providing leadership and direction regarding establishment, implementation, and administration of a viable CM Program for the CMS enterprise; and
- Assisting CMS' Business Owners/Partners, System Owners/Managers, and the Office of Information Services (OIS) in understanding their CM responsibilities and ensuring that they incorporate an acceptable level of configuration control into their projects, products, or automated systems.

5.B. Office of Information Services (OIS)

The OIS (or its identified Designee) is responsible for the following activities:

- Developing and implementing processes, procedures, and standards to ensure compliance with Section 4 above;
- Facilitating implementation of this policy, including providing appropriate training to ensure adherence to this policy;
- Monitoring adherence to this policy and reporting status to the CIO;
- Assisting System Developers, System Maintainers, and Project Owners/Managers with the development of CCB charters and operating procedures;
- Approving all established CCB charters and operating procedures;
- Coordinating and integrating activities of all CMS organizations working CM issues to optimize efficiency and eliminate redundant and/or contradictory efforts;
- Receiving, testing, and evaluating proposed mission unique or site unique CIs that may impact the CMS operational environment; and
- Performing configuration audits and following-up as necessary on identified corrective actions.

5.C. Business Owners/Partners, System Owners/Managers, and Project Owners/Managers

CMS' Business Owners/Partners, Project Owners/Managers, and System Owners/Managers are responsible for the following activities:

- Ensuring that CM activities are planned, coordinated, implemented, and managed for IT projects, products, or automated systems under their control in accordance with the CMS CM policy, processes, procedures, and standards established within the CMS Integrated IT Investment & System Life Cycle Framework;
- Contributing to the identification and control of CIs associated with their IT projects, products, or automated systems;
- Receiving CIs associated with their IT projects, products, or automated systems in accordance with established contractual agreements and management practices;
- Establishing a CCB when appropriate, and ensuring that an approved charter and operating procedures exists for the established CCB;

- Ensuring that cost, schedule, and performance aspects of change requests, problem reports, and engineering change proposals are known at the time of their consideration by the respective CCB; and
- Participating in configuration audits.
- Ensuring that a back-up and restore strategy is documented.

5.D. System Developers and System Maintainers

System Developers and System Maintainers are responsible for the following activities:

- Ensuring that CM activities are planned, coordinated, implemented, and managed for IT projects, products, or automated systems under their control in accordance with the CMS CM policy, processes, procedures, and standards established within the CMS Integrated IT Investment & System Life Cycle Framework;
- Contributing to the identification and control of CIs associated with their IT projects, products, or automated systems;
- Ensuring baseline configurations are adequately documented and maintained;
- Classifying and analyzing change requests and problem reports to determine where resources are concentrated;
- Providing configuration status accounting reports to the appropriate personnel to report up-to-date status of baselined deliverables; and
- Participating in configuration audits.

5.E. Configuration (or Change) Control Boards

CCBs are responsible for the following activities:

- Ensuring that change requests, problem reports, engineering change proposals, or evolutionary builds are processed, evaluated, and adjudicated in a timely manner; and
- Evaluating the scope, applicability, and effect of proposed changes, focusing on the items that affect cost, schedules, or compliance with technical requirements, and providing approval/disapproval based on defined strategic initiatives, program business objectives, and budgetary parameters.

6. APPLICABLE LAWS/GUIDANCE

The following laws and guidance are applicable to this policy:

- Clinger-Cohen Act of 1996 (formerly called Information Technology Management Reform Act (ITMRA), Division E, National Defense Authorization Act for FY 1996 (P.L. 104-106), February 10, 1996
- HHS IRM Guidelines for Capital Planning and Investment Control, HHS-IRM-2000-0001-GD, January 8, 2001, (especially Guideline A: Model Process, 3.4. Configuration Management and Guideline G: The Capability Maturity Model)

- IEEE Standards - Software Engineering, Volumes I-IV, 1999 Edition, Institute of Electrical and Electronics Engineers (IEEE)/Electronic Industries Association (EIA)
- CMS Target Architecture, CMS-CIO-STD-ARC01, Centers for Medicare & Medicaid Services, September 2004
- CMS Integrated IT Investment & System Life Cycle Framework (CMS Intranet and Internet Websites)

7. EFFECTIVE DATES

This policy becomes effective on the date that CMS' Chief Information Officer (CIO) signs it and remains in effect until officially superseded or cancelled by the CIO. This policy supersedes any previous policies issued regarding configuration management.

8. INFORMATION AND ASSISTANCE

Contact the CM Program Manager within the CIO Planning, Management, & Support Group (PMSG) of the Office of Information Services (OIS) for further information regarding this policy.

9. APPROVED

/s/ 8/23/05

D. Dean Mesterharm
CMS Chief Information Officer and
Director, Office of Information Services

Date of Issuance

10. ATTACHMENTS

There are no documents that currently augment this policy.

11. GLOSSARY

Automated System

A configuration of hardware and software infrastructure, applications, and associated documentation, either custom designed or commercial off-the-shelf (COTS) software, or combination thereof, that automates the activities of collecting and/or accessing data or information and performing logical computations in support of CMS' processes.

Baseline

(1) A specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development, and that can be changed only through formal change control procedures. (2) A document or a set of such documents formally designated and fixed at a specific time during the life cycle of a configuration item. (3) Any agreement or result designated and fixed at a given time, from which changes require justification and approval. (IEEE Std. 610-12-1990) A baseline is a configuration identification formally designated and applicable at a specific point in the life cycle of a configuration item.

Build

An operational version of a system or component that incorporates a specified subset of the capabilities that the final product will provide. (IEEE Std. 610-12-1990)

Capability Maturity Model (CMM)

Developed and maintained by the Software Engineering Institute at Carnegie Mellon University, the CMM is a framework that describes the key elements of an effective software development process arranged into five maturity levels: initial, repeatable, defined, managed, and optimizing. Each maturity level indicates process capability and contains a number of key processes directed at achieving goals for planning, engineering, and managing software development and maintenance organized by common features, which address implementation and themselves contain key practices that describe activities or infrastructure. The CMM describes an evolutionary improvement path from an ad hoc, immature process (level 1) to a mature, disciplined process (level 5) that establishes a basis against which an organization can judge, in a repeatable way, the maturity of its software process and compare it to the state of industry practice. The CMM enables a software development organization to consciously choose a certain target level of maturity, and then work towards achieving that level.

Configuration

The functional and physical characteristics of hardware or software as set forth in technical documentation or achieved in a product. (IEEE Std. 610-12-1990)

Configuration Audit

A functional configuration audit is conducted to verify that the development of a configuration item has been completed satisfactorily, that the item has achieved the performance and functional characteristics specified in the functional and allocated configuration identification, and that its operational and support documents are complete and satisfactory. A physical configuration audit is conducted to verify that a configuration item, as built, conforms to the technical documentation that defines it. (IEEE Std. 610-12-1990)

Configuration Control

An element of CM, consisting of the evaluation, coordination, approval or disapproval, and implementation of changes to configuration items after formal establishment of their configuration identification. (IEEE Std. 610-12-1990)

Configuration (or Change) Control Board (CCB)

A group of people responsible for evaluating and approving or disapproving proposed changes to configuration items, and for ensuring implementation of approved changes. (IEEE Std. 610-12-1990)

CCB Charter

A document that defines the purpose, objectives, authority, membership, and responsibilities of an established CCB.

Configuration Identification

An element of CM, consisting of selecting the configuration items for a system and recording their functional and physical characteristics in technical documentation. (IEEE Std. 610-12-1990)

Configuration Item (CI)

An aggregation of hardware, software, or both, that is designated for configuration management and treated as a single entity in the configuration process. (IEEE Std. 610-12-1990)

Configuration Management (CM)

A discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements. (IEEE Std. 610-12-1990)

Configuration Status Accounting

An element of CM, consisting of the recording and reporting of information needed to manage a configuration effectively. This information includes a listing of the approved configuration identification, the status of proposed changes to the configuration, and the implementation status of approved changes. (IEEE Std. 610-12-1990)

IT Project

A temporary endeavor undertaken to create a unique information technology product, service, or result (e.g., an automated system).

Product

A physical entity (e.g., a piece of hardware or software) or artifact (e.g., a document) that is created by someone or some process.