CHAPTER 4, PART 1
CM POLICY & RESPONSIBILITIES

1 BACKGROUND

Configuration Management (CM) is a control activity applied to the components of an Information Technology System throughout its life to provide assurance that the system components are well defined and cannot be changed without proper justification and full knowledge of the consequences. CM ensures that the hardware, software, communications services and documentation for a system can be accurately determined at any time. The term "configuration" is used repeatedly in this document. Configuration means the functional and/or physical characteristics of system as specified in the technical documentation and realized in a product. It includes all of the characteristics of the system that must be controlled: its content, the content of documents that describe it, the versions of the system, system modification documents, data needed for operation of the system, and any other essential elements or characteristics that comprises the system.

a CM Objectives. The objectives of CM are to:

(1) Provide controls to ensure the system operates correctly throughout its life;
(2) Ensure that the configuration of all system components is available and accurate at all times;
(3) Ensure the pertinent functional and physical interfaces between systems, equipments, and software are correctly and adequately documented;
(4) Provide maintenance efficiency by ensuring that change proposals are adequately acted upon; and
(5) Ensure that the impact of any change to system functionality, security, performance, and cost is known at the time the change is approved.

Applying CM to an IT system can enhance a system's cost-effectiveness and security. Changes to the system, when controlled, are less error prone and therefore less costly to complete. Early identification of the impact of a modification on other components can result in better-designed changes. The need for formal approval of change requests will lead to better developed and properly justified changes. The

application of rigorous CM procedures also reduces the risk of malicious changes by making each change to the system visible and ensuring full accountability and audit.

Development of proper configuration documentation provides better control over IT assets. Troubleshooting will be simplified by having available accurate system documentation. Recovery from a disaster or loss of an asset is simplified by having a clear statement of each component and its configuration state. Reversion from a troubled upgrade to a previously stable state is also facilitated. A CM system may also provide useful asset management information, such as component maintenance costs and license fees, appropriate to system financial planning.

From a security perspective, all USDA General Support Systems (GSS) and Major Software Applications (MSA) are required to undergo a security certification process and be accredited by a Designated Accrediting Authority (DAA) prior to being placed in operation. This individual is the agency management official who formally authorizes a system's operation in writing and explicitly accepts any risks associated with that system. The implementation of a formal CM process is a requirement for system accreditation. The documentation maintained for CM will also provide the necessary evidence to the DAAs that the security aspects of each change since the system's last accreditation review have been properly evaluated. This will substantially simplify the re-accreditation process. All systems must be re-accredited any time a major change is implemented.

During the development phase of the lifecycle of a GSS or MSA, requirement and design specifications, test plans/results, Trusted Facilities Manual (TFM), and other technical and support documents must be produced. These documents are incrementally formulated during the development process and subjected to change control. A Configuration Control Board (CCB) reviews and approves developed changes to these products.

The control of CM rests with a body of qualified individuals known as a Configuration Control Board (CCB). The primary function of a CCB is to approve the baseline CM documentation, ascertain all of the benefits, risks and

impacts of changes before a decision is made to implement, defer or reject a change, and schedule new releases of systems. The USDA will implement a two level CCB structure. The first or top level CCB will be an Agency or Site Level CCB chaired by Agency Chief Information Officer (CIO), Agency Heads or Site Executives functioning as their organization's CM Authority (CMA). This level CCB will primarily address business decisions regarding proposed changes related to cost, schedule, and system functionality. The second level CCB will be project or system Level CCBs chaired by project or system managers functioning as their system Configuration Control Authority (CCA). This level CCB will address technical decisions regarding proposed changes to common data structures, design changes, and changes to specific schedules for partial functions, cost, and interim delivery dates within their scope of authority. The scope of authority of each project or system level CCB is derived via a written charter approved by an agency or site level CCB.

Prior to transitioning to operation, these systems and their accompanying documentation are again reviewed and subjected to the security certification process. The certification process is performed to assure the DAA that the system has attained a specified level of security suitable to be accredited for secure operation. The certification process also includes auditing of the technical and support documentation to ensure that all approved changes have in fact been implemented as required.

During the operation and maintenance phase, certified systems remain under change control. Major and/or minor changes to these systems may introduce security vulnerabilities that would require the system to be re-certified. Operational system changes may also generate significant changes to contingency plans, risk assessments, or other accreditation documentation. Therefore, any changes to the system while in operation will continue to be subject to scrutiny and approval by a CCB or its designated representatives.

CM is the process that provides the DAA assurances that changes to these systems have been, and will in the future, be made in a systematic and disciplined manner and that

the system in operation (including its supporting documentation) is the correct version (configuration).

Consequently, a requirement for security accreditation of GSS and MSA systems is that they be developed and maintained with a documented CM process. As a result, assurance in the form of a CM Plan (CMP) is required to satisfy the DAA that the system and it's supporting documentation were developed using a defined CM process and the system will be maintained in accordance with a documented CM process.

The CM process ensures that any changes to be made to these systems will be reviewed and approved by a proper management authority for the system in terms of data confidentiality, integrity, and availability as well as other security implications. Data integrity is a requirement that information and programs are changed only in a specified and authorized manner. System integrity requires that a system perform its intended function in an unimpaired manner, free from deliberate, inadvertent or unauthorized manipulation.

The components of a system that are controlled by the CM process include system technical documentation, code, data, infrastructure items and any other items needed to meet a set of functional requirements (including security requirements) or contractual obligations. The same CM process can control all of these items.

b CM Roles & Functions. There are some roles that are key in an efficient CM process.

(1) CM Authority (CMA): Every IT system is developed and implemented in response to a business need or as a solution to an operational problem. System users define requirements based on their operational needs and ensure that operational user requirements are properly identified, documented, approved, and implemented for all systems under development or being operationally maintained by their organizations. The control of changes to these requirements rests with the Agency Chief Information Officers, Agency Heads or Site Executive acting as their organization's CMA. The

CMA or their designated representative must authorize changes to system requirements.

(2) Configuration Control Authority (CCA): Control of design solutions to meet the needs of operational user requirements rests with the CCA (project or system manager). Control of changes to system design solutions, and the system's accompanying technical documentation, must be approved by the CCA.

(3) CM Specialist (CMS): Someone must manage and operate the CM system: establish detailed procedures, ensure all requests for changes are processed properly, provide reports on the status of all CIs and proposed system changes, and control all of the baseline items. This role is called a CM Specialist (CMS). The individual designated the CMS is critical to the successful operation of a CM system. They are responsible for ensuring that all elements of the CM process are followed and documentation is kept under their physical control.

c CM Major Functions. The five major CM functions are: CM Planning and Management, Configuration Identification, Configuration Change Control, Configuration Status Accounting, and Configuration Auditing and Verification. They are described in detail below.

(1) CM Planning and Management

CM begins with the planning process. CM planning includes planning, coordinating, and managing all of the tasks necessary to implement and conduct CM activities. CM planning and management occurs throughout all life-cycle phases of a system. Documentation of the planning process and development of the CM Plan (CMP) formalizes individual roles and ensures continuity of CM practices at all levels of management.

All agencies and staff offices that develop, operate and maintain USDA systems must develop and implement a CM plan. These plans are subject to review, approval, and implementation prior to the

beginning of the development phase of a system. System or project level CM plans, required for certification and accreditation, must be modified and updated to reflect the current operational or maintenance environment prior to releasing the system to operation.

(2) Configuration Identification

The Configuration Identification process is the foundation for all other CM processes. It documents the products of system engineering and the approved configuration of the physical and functional characteristics of the system or product. In addition, Configuration Identification provides unique product and document identifiers and establishes baselines for Government and contractor configuration control. It also creates records in the status accounting database, supports configuration audit and verification and provides management of system interfaces.

In the Configuration Identification Process any piece of hardware, software, or both that satisfies an end use function and is designated for separate CM is referred to as a Configuration Item (CI). For example, if a system contains several software application programs, each program, and its related documentation and data might be designated a CI. There is no clear and definable definition for what makes up a CI. The number and composition of CIs designated in a system is a design decision. A CI that is purely software is called a Computer Software Configuration Item (CSCI). A CI that is purely hardware is called a Hardware Configuration Item (HWCI). Generally, in USDA, the term CI is used to denote a system such as a Local Area Network (LAN) or a computing platform, which would be composed of both hardware component CIs and/or software
component CIs, either of which, could be a Commercial Off The Shelf (COTS) component. Although the concepts for both hardware and software CM are similar, the software CM process must be more rigorous and deeply imbedded in the engineering process. This is necessary since software is

much more flexible than hardware and therefore much more vulnerable to security exploitation.

As a CI goes through its development process, more and more of its components are developed until the final CI is available for use. Generally, the system life cycle process will first result in a set of requirements, then a design, then product creation, and product testing. The product design, creation, and testing process are usually referred to as the development life cycle, which is a subset of the normal system life cycle. The definition of CM contains the concept of identifying the configuration of each CI at discrete points in time during the life cycle process, and then managing changes to those identified configurations.

The configuration of a system at a discrete point in time is known as a baseline. Thus, a baseline is the documentation, hardware, and software that make up a CI at a given point in its life cycle. Each baseline serves as a point of departure or reference for the next life cycle stage. In the USDA standard life cycle, baselines are established after each life cycle phase at the completion of the formal review that ends the phase.

(3) Configuration Change Control

The configuration change control process manages the current configuration baseline, which results from the configuration identification process. The types and levels of documentation subject to Government configuration control authority are defined in the CM plan.

Each baseline is subject to configuration control and must be formally updated to reflect approved changes to the CI or system as it goes through the life cycle stages. At the end of a life cycle phase, the previous baseline plus all approved changes to it become the new baseline for the next stage. The term "baseline management" is often used to describe this control process.

Normally, the first baseline consists of an approved system requirements document and is known as the "requirements baseline". Through the process of establishing the requirements baseline, the functional and system prerequisites become the explicit point of departure for system development, against which changes can be proposed, evaluated, implemented, and controlled. The requirements baseline is also the basis against which the system is authenticated.

A CM librarian or CM tool administrator stores and controls the contents of software code and system technical documentation in a location called a Program Library. This library must contain the official master copies of all configuration items baselines or pointers to their location. It contains all item's code and object module baselines. These baselines are checked out by the librarian for authorized changes to be made and are checked back in after the change is complete. CM program libraries may be established at the office, agency, site, or system program/project organizational level. Efficient operation of the library is enhanced if automated tools are available.

The program library is usually under the control of the CM Specialist (CMS). Depending on the size of the system being developed or maintained, the CM librarian or CM tool administrator may be assigned as a collateral duty for the CMS, system administrator, or other system project personnel. However, if these duties are assigned as collateral, then system managers must be aware of the threat to system security as it relates to separation of duty vulnerabilities.

A CCB will be the official agency forum used to establish CM baselines and to recommend subsequent changes to those baselines. CCB charters and operating procedures may be created as separate independent entities or included in the CM plans and procedures documents. Proposed changes to system baselines must be submitted to the appropriate CCB.

A decision-making authority, CMA or CCA depending on their scope of control, approves or disapproves

proposed changes and exercises control via a CCB. A CCB is chaired by a CMA or CCA, who can authorize the expenditure of resources. Other members are chosen based on their ability to provide advice on the costs and benefits of a change. Usually under the CCB rules of operation, the chair unilaterally decides the disposition of the proposed changes after receiving the advice of the other members. The CCB process is facilitated by the CMS, who provides the requests for changes and the associated analysis of impact. In addition, the CMS records the decisions of the CCB and provides them to the change requester or individuals who will implement the change.

Approved changes are typically grouped for implementation to reduce the number of configurations supported in the field. All documentation (operator manuals, maintenance data, programmer manuals, training materials, engineering data, specifications) is updated to reflect design changes and is made available concurrently with implementation of the change.

(4) Configuration Status Accounting (CSA)

All other processes provide information to the Configuration Status Accounting (CSA) database, as a by-product of transactions that take place, as the CM functions are performed. This process provides visibility into status and configuration information concerning the product or system and its documentation. CSA should provide a track of configuration documentation changes and document the configuration of items. These records should include both current and historical information to ensure trace-ability from the initial requirements or previous baseline.

Any CM Automated Information System (CM AIS) database should provide such information as the designed, built, delivered, or modified configuration of any serially numbered end item and any serially numbered component, to the extent consistent with the organization's maintenance support strategy. Using CSA, project managers/others can determine the

current status of any change, the history of any change, the schedules or status of verifications and audits, as well as resultant action items. Metrics (performance measurements) are obtained from the information in the CSA database. This information can be used to monitor and improve the CM process.

(5) Configuration Audit and Verification

The Configuration Audit and Verification process is used to verify that a product's performance requirements have been achieved by the product/system design and accurately documented. This process considers information from the CSA database, results of product/system testing, the physical hardware or software (or its representation) and the software engineering environment to perform this verification. In addition, it ensures that the product design has been accurately documented in the configuration documentation. This process also includes verifying the incorporation of approved changes.

Configuration verification should be an imbedded function of the process for creating or modifying the product. Successful completion of verification and audit activities result in a verified product and documentation set that may be confidently considered a Product Baseline. In addition, configuration verification is a validated process that will maintain the continuing consistency of product documentation.

2 POLICY

All USDA agency CIOs, Agency Heads and Site Executives will implement an effective CM program that provides overall guidance and procedures for all Information Technology (IT) systems under their control. This policy applies to all IT systems under development and to existing operational systems regardless of where they are in the life cycle. All agencies and staff offices will incorporate general CM requirements in all Statements of Work (SOW) and procurement requests for all IT contracts that involve

USDA systems. This policy will be implemented within 180 days from the issuance of this notice.

Policy Exception Requirements – Agencies will submit all policy exception requests directly to the ACIO for Cyber Security. Exceptions to policy will be considered only in terms of implementation timeframes; exceptions will not be granted to the requirement to conform to this policy. Exceptions that are approved will be interim in nature and will require that each agency report this Granted Policy Exception (GPE) as a Plan of Action & Milestone (POA&M) in their FISMA reporting, with a GPE notation, until full compliance is achieved. Interim exceptions expire with each fiscal year. Compliance exceptions that require longer durations will be renewed on an annual basis with a updated timeline for completion. CS will monitor all approved exceptions.

3 PROCEDURES

All IT project or system managers will establish and implement a CM program that provides overall guidance and procedures for their systems. A Configuration Control Board (CCB), with an approved Charter and Operating Procedures, will be the official agency forum used to establish CM baselines and to recommend subsequent changes to those baselines. Each CCB will be chaired by the CCA, a senior manager (often the project manager or system manager), who can authorize the expenditure of resources and make decisions.

Agencies that manage large computing facilities, such as the National Finance Center (NFC) and the National Information Technology Center (NITC), will develop and implement site CM programs, which include the development of Site CM Plans and procedure documents. Site CM Plans/procedures include all IT systems managed within the facility. Agencies with systems that do not use large computing facilities are required to create individual CM plans and procedures to augment those developed at the agency-wide level. This will ensure that CM plans and procedures are developed for each IT system under an agency's control.

Offices and agencies will provide a Management Plan signed by their CIO or IT Management Official describing the CM program they have implemented or a Plan Of Action & Milestones (POA&M)

describing their approach to developing and implementing the required CM program. This plan will be submitted to the Associate CIO for Cyber Security within 90 days from the issuance of this notice.

4 RESPONSIBILITIES

a The USDA Chief Information Officer and Deputy CIO will:

Promote and support an effective program of Configuration Management for all USDA Information Technology (IT) Systems.

b The Associate Chief Information Officer for Cyber Security will:

(1) Ensure that CM is implemented on all new and existing information systems and networks that process, store, communicate or provide access to Classified or Sensitive But Unclassified (SBU) information;
(2) Evaluate and report on agency or mission area compliance with this directive to the CIO during periodic security reviews and evaluations;
(3) Review all exception requests for extended CM implementation time and provide a prompt response;
(4) Maintain a database of all IT systems with current information on the agency or mission area progress toward the implementation of a formal CM program; and
(5) Provide expert assistance and training to agencies or mission areas to aid in establishing an effective CM program.

c The Associate Chief Information Officer for IRM will:

(1) Collaborate with the Office of Cyber Security in supporting CM Policy;
(2) Receive, review and participate in the joint review of all exceptions requests for extended CM implementation time; and
(3) Assist agencies and mission areas in obtaining ANSI/EIA standard licensing agreements on a departmental basis.

d Agency Chief Information Officer will:

(1) Act as the CM Authority (CMA) or Configuration Control Authority (CCA), as appropriate, for all IT systems developed or maintained under their purview;
(2) CMAs will assign CCAs and authorize and charter subordinate Configuration Control Boards (CCBs) with the authority to manage and oversee the CM activities for Information Technology (IT) Systems being developed or maintained by their organizations;
(3) Act as or delegate an individual as the chairperson for all CCBs meetings conducted;
(4) Develop and implement a CM system within their organizations;
(5) Agencies and staff offices will ensure that a requirement for adherence to agency CM plans and procedures is incorporated in all SOWs and procurement requests for IT systems;
(6) Assign a CMS to manage the development, implementation and maintenance of their respective CM system;
(7) Publish and distribute internal policies and procedures to implement this policy within the organization to include personnel who develop, maintain, and install USDA IT systems;
(8) Provide adequate resources and funding to perform CM activities;
(9) Train all personnel responsible for CM in the objectives, procedures and methods of performing this process; this includes system developers, project engineers, system administrators, system engineers, acquisition officials and others involved in management of IT systems;
(10) Prepare an office, agency, site, project, or system specific CM Plan for all new and existing information systems and networks that process, store, communicate or provide access to Classified or SBU information;
(11) Establish a CM Program Library or repository for all system documents and baselines;
(12) Ensure that all subordinate IT System Managers and contractors initiate, record, review, approve and track change requests/problem reports for all configuration

items/elements according to a documented CM process;

(13) Ensure that software products are created from the software baseline library and control their release in accordance with a documented CM procedure;

(14) Identify, control and make available selected system work products for review or audit purposes;

(15) Ensure that affected work groups are informed of the status and content of system baselines;

(16) Control system baselines according to a documented procedure as specified by the CM process;

(17) Establish and use system performance measurements to determine the status of CM activities for all systems;

(18) Ensure reviews and audits are conducted annually of the overall agency CM program by an independent evaluator (independent of the CM group) and report the results to the CIO for Cyber Security;

(19) Provide suggested changes to this policy as appropriate to enhance the overall CM process in USDA;

(20) Prepare a Management Plan for implementation of a CM program for all IT Systems and provide the plan to the CIO for Cyber Security;

(21) Request exceptions for any IT System that requires additional time in which to institute an appropriate CM process;

(22) Make decisions on changes;

(23) Request and evaluate impact assessments;

(24) Give final approval on all changes within jurisdiction;

(25) Assign action items, as required;

(26) Establish criteria for acceptability of proposed changes; and

(27) Keep higher-level management advised of significant changes in design, cost, and schedules.

e The agency Information Systems Security Program Manager (ISSPM)/designate will:

(1) Participate as a member of the Configuration Control Boards (CCB) to ensure that configuration changes are properly controlled and documented for all agency IT systems and that the changes do not harm system security properties;

(2) Provide necessary assistance or guidance in the establishment of a CM program;
(3) Review and provide security input in the development of CM plans;
(4) Identify those IT systems not compliant with this policy and provide this information to the agency CIO or Agency Head;
(5) Provide quarterly input to agency senior management officials on the progress of CM activities for all IT systems; and
(6) Offer input to impact assessments, as required.

f Other CCB Members:

(1) Attend CCB meetings, as required;
(2) Express and coordinate their organization's viewpoints at meetings;
(3) Review and evaluate all change requests and data packages before attending the CCB meetings;
(4) Communicate with other members of the CCB regarding changes;
(5) Provide input to impact assessments as required; and
(6) Be prepared to negotiate for the component represented and have authority to commit the organization to take action on the changes being reviewed.

g Agency CM Specialist (CMS)/Designate will:

(1) Implement the applicable organizational CM Program and CM requirements baselines for all agency/site IT systems;
(2) Establish and maintain a CR tracking database;
(3) Develop and publish the organization's CM Plan and operating procedures;
(4) Develop and review CCB Charters, as required;
(5) Act as secretary to the applicable organizational CCB by preparing and distributing its agendas and minutes, recording status of CRs effected by CCB deliberations and preparing project change authorizations for CCB approved
CRs;
(6) Produce and distribute periodic database, individual system or product CR status reports;

(7) Support developer functional and physical configuration audits (FCA & PCA);
(8) Review CM Plans for conformance to requirements;
(9) Coordinate CRs with other individuals responsible for implementation of approved changes (gate keeping); and
(10) Resolve all CR problems to promptly mitigate system/product impact.

h CM Librarian (CML)/Tool Administrator will:

(1) Manage the SCM library and thereby control the use and revision of official copies of baseline components;
(2) Administer and maintain CM tool suite(s) as appropriate; and
(3) Ensure that all baseline revisions have been approved and signed by the CCA.

-END-