ADMINISTRATIVE COMMUNICATIONS SYSTEM
UNITED STATES DEPARTMENT OF EDUCATION
Office of Management, Executive Office
400 Maryland Avenue; Washington, DC 20202

Transmittal Sheet #:	2005-0011	*Date:*	July 12, 2005
Distribution:	All ED employees	*Distribution Approved:* *Directives Management Officer:*	/s/ Tammy Taylor

Action: Pen and Ink Changes

Document Changing: Handbook OCIO-11, *Handbook for Information Technology Security Configuration Management Planning Procedures*, dated 05/13/2003

Summary: This *Handbook for Information Technology Security Configuration Management Planning Procedures* provides a comprehensive and uniform approach to developing a configuration management plan for every Department General Support Systems and Major Applications.

Pen and Ink Changes: The following pen and ink changes were made.

Page	*Section*	*Changed*	*To*
All	Date	05/13/2003	07/12/2005
1	Superseding Information	Information described above	Information described above
All	All	Several corrections were made to the document including formatting changes, punctuation changes, and title changes. No technical changes were made to the document.	

ADMINISTRATIVE COMMUNICATIONS SYSTEM
UNITED STATES DEPARTMENT OF EDUCATION

Handbook

Distribution:
All Department of Education Employees

Approved by: /s/ (05/13/2003)
William J. Leidinger
Assistant Secretary
Office of Management

Handbook for Information Technology Security Configuration Management Planning Procedures

For technical questions concerning information found in this directive, please contact Kathy Zheng on (202) 245-6447 or via e-mail.

Supersedes Handbook OCIO-11, Handbook for Information Technology Security Configuration Management Planning Procedures, dated 5/13/2003.

U.S. DEPARTMENT OF EDUCATION
INFORMATION TECHNOLOGY SECURITY

Handbook for Information Technology Security Configuration Management Planning Procedures

July 2005

Table of Contents

1. INTRODUCTION

1.1 Purpose

This *Handbook for Information Technology Security Configuration Management Planning Procedures* provides a comprehensive and uniform approach to developing a configuration management plan (CMP) for every U.S. Department of Education (Department) General Support Systems (GSS) and Major Applications (MA)[1]. The handbook provides guidance to the individuals responsible for, or involved in the configuration management (CM) of Department GSSs and MAs, who may also be responsible for developing a CMP that is compliant with the Department's minimum standards.

1.2 Background

CM is the process of establishing and maintaining the technical integrity of a system throughout its life cycle by systematically identifying, controlling, and accounting for all changes made to a system. According to the *Handbook for Information Assurance Security Policy*, a CM process shall be developed for each GSS/MA to effectively manage and track system changes. As part of the documentation required for a GSS or MA to be certified and accredited, the *Handbook for Information Technology Security Certification and Accreditation Procedures* requires a CMP as one of the security documents that must be developed.[2] This handbook provides a structured method of documenting the CM process for a GSS/MA in a CMP.

1.3 Scope

This handbook outlines the major elements of a CMP and provides a description of the content that should be included in each section. In addition, the handbook provides a high-level introduction to CM and CMPs, including what CM is, what a CMP is, and why and when a CMP should be developed. The handbook also describes, in depth, the configuration control process (CCP), which is the most important element of the CMP.

This handbook is based on the *Handbook for Information Assurance Security Policy*; Office of Management and Budget (OMB) Circular A-130, *Appendix III, Security of Federal Automated Information Resources*; and other applicable Federal information technology (IT) security laws and regulations.

1.4 Structure

This handbook is organized into five (5) major sections:

- **Section 1** provides an introduction to the procedures;
- **Section 2** provides a high-level introduction to CM and CMPs;
- **Section 3** describes the key elements of a CMP;

---

1 *The Handbook for Information Technology Security General Support Systems and Major Applications Inventory Procedures* can be used to help determine if a particular system is a GSS or MA.

2 For more information on the Department's certification and accreditation process, refer to the *Handbook for Information Technology Security Certification and Accreditation Procedures*.

- **Section 4** provides an overview of the CCP, a major component of the CMP; and
- **Section 5** provides a summary of the document.

This handbook also includes the following seven (7) appendices:

- Appendix A: Glossary of Terms;
- Appendix B: Acronyms;
- Appendix C: References;
- Appendix D: Sample Change Request Form;
- Appendix E: Sample Security Impact Assessment Form;
- Appendix F: Sample Emergency Change Request Form; and
- Appendix G: Sample Change Request Status Log.

2. CONFIGURATION MANAGEMENT

2.1 What is Configuration Management?

CM is defined as the systematic identification, documentation, and control of system elements by recording and reporting change processing and implementation status. These activities assist in verifying compliance with specified system requirements as well as establishing and maintaining the technical integrity of a system throughout its life cycle. The successful implementation of CM activities results in an established and documented system baseline[3], effective management and tracking of changes made to a GSS/MA and related documentation (version control), and effective risk management.

2.2 What is a Configuration Management Plan?

A CMP is a living document that identifies CM roles and responsibilities, resources, and formal processes and procedures to ensure that all proposed changes to a GSS/MA are evaluated and approved before implementation. This plan is essential for effective CM pertaining to activities such as system-wide upgrades, replacements, and deployments. In addition, it is a key process for maintaining the appropriate level of information security for a GSS/MA.

A CMP should include and address CM roles and responsibilities, communications, system configuration baseline, configuration control process, and CM resources. In addition, the plan should also include a cover page and table of contents, an executive summary, and an introduction section. A detailed description of each CMP component is provided in *Section 3*.

2.3 Why Develop a Configuration Management Plan?

Based on OMB A-130, the *Handbook for Information Assurance Security Policy*, and other Federal laws and regulations, a CM process must be developed and documented in a CMP for all GSSs and MAs. Developing a CMP is critical for implementing CM and ensures the following:

- **Changes to the configuration are identified and evaluated to determine the impact to system security before implementation.**

Any changes made to the system are documented and tracked. Ideally, this process begins at the system development stage and is carried out until the system is replaced. Because each change is tracked from initial system development through completion, a thorough history of changes is created for that system. For example, an MA running on an Oracle database may require an upgrade to a more recent version of Oracle because of existing vulnerabilities in the older version. Upgrading to the more recent version of Oracle will change the MA's configuration. The need for a version upgrade is a configuration change that must be thoroughly analyzed, since it may affect security, system performance, and functionality. This change should be documented in a formal process to provide a historical representation of one of the changes occurring throughout the system development life cycle (SDLC).

[3] *System baseline will be discussed in detail in Section 4.*

- **Configuration is documented ensuring that version control is maintained. Upgrades and additions are easily implemented because of hardware and software controls in a formal CM process.**

The system documentation includes information on the system specification and configuration design, ensuring that, as part of the CMP, system documentation can be checked to verify whether the designed configuration allows the system to achieve its objective. For example, if an MA's system design needs to be modified to implement a stringent password for users, it could be determined that this change will be included in a later version. Prior to the new version's implementation, all changes should be documented to ensure that version control is maintained.

- **The configuration is verified against the initial baseline ensuring that all changes have been maintained and documented for any new parties involved in the CM process.**

Information on the system, including the manufacturer, model type, and software version, is recorded and tracked, ensuring access to the most recent system information.

2.4 When Should a Configuration Management Plan be Developed?

Ideally, a CMP should be developed at the beginning of the SDLC to ensure that a CM process is established to control, track, and maintain all changes that are made to the GSS or MA throughout the SDLC. A CMP is a living document and should be reviewed and updated as needed—at least annually—throughout the entire SDLC. It is possible to develop a CMP after the system has been deployed; however, existing system documentation (i.e., system security plan, system configuration documents, system maintenance records, vendor manuals, system configuration diagrams, and security-related information) will be more heavily emphasized in the development of the CMP.

3. CONFIGURATION MANAGEMENT PLAN COMPONENTS

This section provides a detailed description of each CMP component and the type of information that should be included in each section. The CMP components are as follows:

- Cover Page;
- Table of Contents;
- Executive Summary;
- Introduction;
- Roles and Responsibilities;
- Communications;
- System Configuration Baseline;
- Configuration Control Process;
- CM Resources; and
- Appendices.

3.1 Cover Page

The cover page should include specific information to identify the document, including the GSS/MA name, Principal Office (PO), title, version number, and date.

3.2 Table of Contents

The table of contents should provide an outline of the CMP sections, subsections, and appendices with page numbers for each.

3.3 Executive Summary

The executive summary should provide a high-level synopsis of the contents included in the CMP.

3.4 Introduction

The introduction should, at a minimum, include the purpose, scope, and structure of the CMP.

3.5 Roles and Responsibilities

This section should clearly identify CM roles and responsibilities for the GSS/MA, noting that all CM activities should be performed in accordance with the processes and procedures documented in the CMP. Some examples of CM roles and responsibilities within an organization are provided in *Table 3-1*.

Table 3-1. Configuration Management Roles and Responsibilities

Role	Responsibilities
Chief Information Officer	The Chief Information Officer (CIO) is responsible for setting forth policies regarding CM and implementing CM at the highest level for the Department.
System Owner/Manager	The system owner/manager or other designated individual serves as the authority for all matters of CM for the GSS/MA. The system owner/manager is responsible for developing functional requirements and verifying that the requirements are implemented appropriately. This individual may also play a role in establishing the Configuration Control Review Board (CCRB) and may be involved in the selection of the CCRB members.
CM Manager	Each GSS/MA should have a CM manager assigned to oversee all aspects of the CMP. The CM manager is responsible for all day-to-day activities necessary to support the CMP and may call on other personnel for assistance. The main responsibilities of the CM manager are to: ▪ Implement the CMP ▪ Provide operational support to the CCRB ▪ Draft the CMP for CCRB approval ▪ Provide the CCRB with information to evaluate changes and screen materials ▪ Arrange CCRB meetings, provide agendas, and prepare meeting minutes ▪ Coordinate implementation of CCRB decisions ▪ Maintain CM Library and database ▪ Coordinate CMP with other security documentation, as required.
CM Librarian	The CM librarian is appointed by the CM manager and is responsible for storing, retrieving, and distributing CM library materials.
Configuration Control Review Board	The CCRB is the governing body for CM policy and guidance affecting all GSSs and MAs within the organization. A chairperson should be appointed by the CCRB to oversee the activities of the Board. The main responsibilities of the CCRB include: ▪ Managing CM operations ▪ Reviewing and approving the CMP ▪ Evaluating, approving, or disapproving change requests ▪ Ensuring proposed changes are limited to those necessary to correct deficiencies ▪ Satisfying changes in operational capability, personnel safety, and logistics support requirements ▪ Effecting substantial life-cycle cost savings ▪ Maintaining security requirements ▪ Preventing slippages to approved schedules ▪ Ensuring proposed changes do not adversely affect external systems, subsystems, facilities, software, or services ▪ Establishing system baselines and authorizing changes to applications
System Users	System users are responsible for reporting any weaknesses that are identified in current versions of the hardware, software, and components.
Other Roles	Other roles within the PO, such as the computer security officer (CSO), system security officer (SSO), and system administrator, may also have specific CM responsibilities. Once the extent of these responsibilities is determined, they should be documented within the CMP for the GSS / MA.

3.6 Communications

The communications section should discuss the methods used to share information regarding CM (e.g., upgrades, application changes, technical notices, and version control). This section should address items such as who has access to the information and how, when, and what type of information is shared.

3.7 Configuration Control Process

This section should identify the CCP that is required to ensure all changes to the GSS/MA are properly requested, evaluated, and authorized. The CCP should provide detailed, step-by-step procedures for establishing, processing, tracking, and documenting changes. At a minimum, the following eight (8) basic steps should be included in the CCP:

- Step 1: Establish System Configuration Baseline;
- Step 2: Identify Change and Complete Change Request Form;
- Step 3: Submit Change Request Form;
- Step 4: Evaluate Change Request Form;
- Step 5: Review Impact Analysis;
- Step 6: Approve, Disapprove, Defer, or Refer Change Request;
- Step 7: Perform Configuration Status Accounting; and
- Step 8: Conduct Configuration Verification and Audit.

Since the CCP makes up the largest section in the CMP, *Section 4* Configuration Control Process will provide further details on the eight steps listed above.

3.8 Configuration Management Resources

The CM resources section of the CMP should describe facilities and tools used for CM activities. This information serves as guidance for planning the resources required to support the functions of each PO throughout the CM process. Because the number of staff, equipment, and space required will vary according to each PO's needs, the CM manager should periodically review the resources involved in CM and verify that the facilities and tools are up-to-date. The CM manager should also work with the system owner and CCRB to determine what type of software package will be best for the organization and its systems.

3.8.1 Facilities

Facilities consist of dedicated spaces for personnel and equipment. Security controls should be in place to safeguard the materials based on confidentiality and sensitivity requirements. This section should include any physical/environmental security controls that must be in place to protect the GSS/MA.

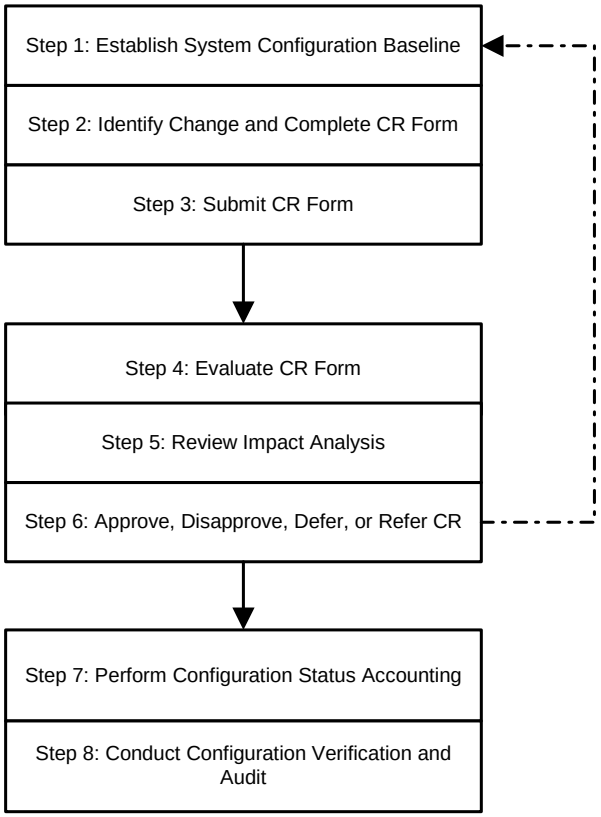
3.8.2 Tools

Using automated tools is an effective way of managing CM activities and maintaining change control. This section should identify any commercial off-the-shelf (COTS) software packages, automated software, or support hardware and software that is used to build and manage the GSS/MA.

4. CONFIGURATION CONTROL PROCESS

The CCP is a critical portion of the CMP because of the number of changes, revisions, upgrades, and modifications that a GSS/MA might undergo throughout its life cycle. Thus, the effective management of changes requires a formal, documented, systematic process for requesting, evaluating, tracking, and approving changes to a GSS/MA. *Figure 4-1* is an illustration of the CCP.

Figure 4-1. Configuration Control Process



The following sections provide a detailed description of the eight minimum steps that should be included as part of the CCP. These steps should be tailored to the needs of the organization and the GSS/MA.

4.1 Step 1: Establish System Configuration Baseline

The first step of the CCP is to establish the System Configuration Baseline, which is a snapshot of the current design and functionality of the GSS/MA, and to provide details regarding all hardware and software. The System Configuration Baseline includes identification of servers, workstations, and software applications that are currently being used in the production environment and the specific configuration settings for each. If the GSS/MA is not yet operational, the System Configuration Baseline should be documented to reflect the current

status of the GSS/MA is within the SDLC. Specifically, the following items should describe and/or identify the System Configuration Baseline:

- System Architecture;
- System Characterization;
- Hardware;
- Software; and
- System Library.

This information may be collected from various system and/or security documentation. The amount of existing documentation may depend on where the GSS/MA is within the SDLC.

4.1.1 System Architecture

A thorough analysis of the system topography should be provided as part of the System Configuration Baseline. A diagram may be needed to depict the system hardware used and any connectivity devices (hubs, routers, and firewalls). The diagram should indicate all connections to other systems and/or networks that are either internal to the Department or external to other organizations.

4.1.2 System Characterization

The system characterization should consist of a description of the GSS/MA, providing information such as:

- Purpose and functionality of the GSS/MA;
- Number of users;
- System criticality and information sensitivity levels;
- System confidentiality, integrity, and availability levels; and
- Type of data that is processed by or stored in the GSS/MA.

If a risk assessment report is available for the GSS/MA, the system characterization of the GSS/MA may be extracted from the report and used in this section.

4.1.3 Hardware

The hardware used to support the GSS/MA should be identified and documented when establishing the System Configuration Baseline. Listed below is information that should be included for each piece of hardware:

- Manufacturer's name;
- Model number;
- Serial number;
- Configuration settings; and
- Hardware specifications, parts, and/or boards.

Additional information, such as vendor support contact information, may also be included as necessary.

4.1.4 Software

The software used to support the GSS/MA should be identified and documented as part of the System Configuration Baseline. Information that should be included for each piece of software includes:

- Title (including acronym or nickname used to reference the software);
- Version number;
- Build number (if appropriate);
- Media (such as 4-mm tape, 8-mm tape, and CD ROM);
- Hardware requirements necessary to run the software (such as available disk space, random access memory, and network connections); and
- Control parameters (password policy, account lockout policy, requirements to change existing passwords, audit policy, user rights assignments, event log policy, restricted groups, system services settings, file permissions settings, etc).

Additional information, such as vendor support contact information, may also be included as necessary.

4.1.5 System Library

This section should include a list of all system documentation and supporting information, as well as a description of the CM library.

4.1.5.1 System Documentation and Supporting Information

All system documentation, such as the following, used to establish the System Configuration Baseline should be referenced:

- User Manuals;
- System Reference Guides;
- System Security Plan;
- Contingency Plan;
- Risk Assessment;
- Security Test and Evaluation (ST&E) Plan; and
- Disaster Recovery Plan (if applicable).

Supporting information, such as the following, should also be included:

- Glossary of terms
- List of acronyms
- Hardware/software inventory
- Project procedures and plans
- Development specifications
- System configuration diagrams[4]
- Personnel staffing requirements
- Project standardization documents
- System or subsystem specifications
- Change request form
- Status accounting

All system documentation and supporting information should include the title, publication date, version number, and revision date of each document, if applicable.

[4] System configuration diagrams help to explain various system components. These diagrams explain how other systems are electronically linked to the system as well as their interconnection of user bases. The diagrams include internal and external connections to the system, and are basically a picture of the system's architecture and links to the system. These types of diagrams can be used as an aid when conducting an inventory of system hardware.

4.1.5.2 CM Library

The CM library should maintain all CM-related documentation (e.g., change request (CR) forms, security impact assessment forms, and CR status log). The CM manager should be responsible for maintaining the CM library to ensure all documents regarding GSS/MA changes are stored in an orderly manner, and copies are provided to authorized persons, when necessary. If the GSS/MA is complex or is frequently updated or changed, the CM manager may delegate some responsibilities to a CM librarian, who is generally responsible for storing, retrieving, and distributing library materials.

4.2 Step 2: Identify Change and Complete CR Form

At some point, a change to the GSS/MA may be needed; thus, this step describes how a CR is initiated and what to do when this occurs. To initiate a change, the need for that change should be identified and other relevant information (such as what type of change it is, why the change is necessary, and how the change may be implemented) should be collected. A change may be categorized as an emergency, major, minor, or optional change. Emergency changes are not typically required to undergo the entire CCP; however, emergency changes must be properly documented and authorized. For an emergency change, an emergency CR form should be completed. The emergency CR form will provide information such as justification, timeframe, and the potential impact on security, including a signature from the approving security official (See *Appendix F* for a sample Emergency Change Request form).

To initiate a nonemergency change, a CR form should be completed. Information provided on the CR form should include the title and description of the change, impact of the change, justification for the change, and estimated number of staff necessary to implement the change. (See *Appendix D* for a sample Change Request form). The system owner or other designated individual should ensure that all information on the form has been completed before submission.

A security impact assessment form should also be included with the CR form, describing in detail the possible impact that this change could have on system security (See *Appendix E* for a sample Security Impact Assessment form).

4.3 Step 3: Submit CR Form

The completed CR form should be submitted to the CCRB for approval. Once the CCRB receives the form, a CR tracking number is assigned to and documented on the CR form. All emergency CR forms should also be submitted to the CCRB for approval within a more critical timeframe and an emergency request number is assigned to and documented on the emergency CR form. In addition, the CCRB should update the CR status log to include all new CRs, including emergency requests, so the change can be tracked (See *Appendix G* for a sample Change Request Status Log).

All GSS/MA configuration changes may not have to be approved by the CCRB. For example, changes to an MA's Microsoft Access database field may not have to be approved by the CCRB. However, the system owner or designated individual must review technical and business analyses to determine how the change will impact the system and render a decision based on the

information provided. All changes should be tracked in either a CR status log or in an equivalent log that maintains all configuration changes.

4.4 Step 4: Evaluate CR Form

In Step 4, the CCRB should carefully evaluate the information provided on the completed CR form to determine whether or not to approve the change. Missing or inadequate information could preclude the CR from being expedited immediately. This section should provide details on how the evaluation is performed and should establish a time frame for decisions to be made regarding regular CRs as well as emergency CRs.

4.5 Step 5: Review Impact Analysis

The CCRB should review the technical and business effects of implementing the change to the GSS/MA. The technical analysis, usually conducted first, should determine the following:

- Whether the change is technically correct;
- Whether the change is technically necessary and feasible within the system constraints;
- How system security will be affected;
- All associated costs for implementing the change; and
- All security components affected (this section will be included in the Security Impact Assessment Form; see *Appendix E*).

The business analysis should determine the following:

- Milestones and if the requested time frames are feasible;
- Whether the change affects an existing contractual agreement regarding the system; and
- Overall impact to the PO, the Department, associated costs with purchasing the hardware, software, and labor as well as the impact on personnel schedules.

The CCRB should take into consideration the results of the impact analysis review before making a decision about the change.

4.6 Step 6: Approve, Disapprove, Defer, or Refer CR

The CCRB should review the CR and impact analysis and make a decision based on the information provided. The CR status log should be used to track all CR's and corresponding decisions. The CCRB has the option to choose one of the following decisions:

- Approve. Immediate implementation is authorized and may occur at any time after an authorized signature has been documented on the CR.
- Disapprove. Immediate denial of the request regardless of circumstances and information provided.
- Defer. Immediate decision is postponed until further notice. This decision could be due to lack of documentation or results of the technical and business impact analyses.
- Refer. A decision cannot be made by the CCRB alone. In this situation, the CCRB may seek consensus with an independent, objective party to ensure that the decision will not drastically affect system security.

4.7 Step 7: Perform Configuration Status Accounting

This step consists of maintaining records of all changes and ensuring the traceability of each CR from initiation through resolution and disposition. Status accounting enables the implementation of approved changes to be tracked and managed and accomplishes the following:

- Provides historical databases and records;
- Provides the status of approved baseline, proposed changes, and implementation of approved status;
- Determines the status on all systems in the CM process; and
- Tracks changes and action items.

4.8 Step 8: Conduct Configuration Verification and Audit

The final step of the CCP is to conduct configuration verification and audits to ensure compliance with the current configuration control requirements. Verification provides the means to examine the characteristics of each system and the supporting documents to verify that the configuration in place meets the user's needs and the current configuration is the approved System Configuration Baseline.

Audits include functional and physical configuration audits. Functional configuration audits verify that the system's actual performance conforms to the stated requirements and physical configuration audits ensure the baseline documentation is a true representation of the "as-built" version of the software and hardware. In addition, as part of the audit process, CM documentation will be verified for accuracy with respect to content and timelines. Verification and audit ensures the following:

- Changes are properly implemented;
- Regulations and standards are followed;
- Documentation is accurate (e.g., test results, vendor documentation, system environment, and configuration identification information);
- The system performs its functions; and
- Security status is constant.

5. SUMMARY

CM is a key process for maintaining the appropriate level of information security for a GSS/MA. In order to manage changes effectively, a formal and systematic set of procedures that describe how to process changes to the system must be developed and implemented. As described in the handbook, the CCP is a critical portion of the CMP that is required to ensure all changes to the GSS/MA are properly requested, evaluated, and authorized. The CCP should include a minimum of the following eight steps, tailored to fit the needs of the GSS/MA:

- Step 1: Establish System Configuration Baseline;
- Step 2: Identify Change and Complete CR Form;
- Step 3: Submit CR Form;
- Step 4: Evaluate CR Form;
- Step 5: Review Impact Analysis;
- Step 6: Approve, Disapprove, Defer, or Refer CR;
- Step 7: Perform Configuration Status Accounting; and
- Step 8: Conduct Configuration Verification and Audit.

These procedures provide a structured method, which is in compliance with the Department's standards for documenting the CM process for a GSS/MA in a CMP, which is required for Certification and Accreditation (C&A). The outcome--a successfully documented CM process--ensures that the GSS/MA has a plan in place for updating, changing, adding, or deleting hardware or software configurations implemented after the initial baseline.

Specific questions or comments regarding the content of this handbook should be directed to the Information Assurance (IA) staff within the Office of the Chief Information Officer (OCIO).

Appendix A. Glossary of Terms

Configuration. Functional and physical characteristics of hardware or software as set forth in technical documentation or achieved in a product.

Configuration Control. The systematic proposal, justification, evaluation, coordination, approval, or disapproval of proposed changes, and the implementation of all approved changes in the configuration after the baseline has been established.

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.

General Support System (GSS). An interconnected set of information resources under the same direct management control that share common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. For example, a system can be a local area network (including smart terminals) that supports a branch office, an agency -wide backbone, a communications network, a departmental data processing center (including its operating system and utilities), a tactical radio network, or shared information processing service organization. See the *Handbook for Information Technology Security General Support Systems and Major Applications Inventory Procedures* for more details.

Major Application (MA). An application that requires special attention to security because of the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. *Note*: All federal applications require some level of protection. However, certain applications, because of the information they contain, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate. See the *Handbook for Information Technology Security General Support Systems and Major Applications Inventory Procedures* for more details.

System Configuration Baseline. A snapshot of the current design and functionality of the GSS or MA, including details regarding system architecture, system characterization, hardware, software, and system library. The current configuration that has been formally reviewed and agreed upon, and thereafter serves as the baseline.

System Development Life Cycle. A structured approach for systems development from planning and support to disposal of the system. A proven series of steps and tasks used to build and maintain quality systems faster, at lower costs, and with less risk.

Appendix B. Acronyms

C&A	Certification and Accreditation
CCP	Configuration Control Process
CCRB	Configuration Control Review Board
CIO	Chief Information Officer
CM	Configuration Management
CMP	Configuration Management Plan
COTS	Commercial off-the-Shelf
CR	Change Request
CSO	Computer Security Officer
Department	U.S. Department of Education
GSS	General Support System
IT	Information Technology
MA	Major Application
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PO	Principal Office
SDLC	System Development Life Cycle
SSO	System Security Officer
ST&E	Security Testing and Evaluation

Appendix C. References

Carnegie Mellon University Software Engineering Institute, *The Capability Maturity Model – Guidelines for Improving the Software Process*, Addison-Wesley, 1994.

DEF STAN 05-57, *Department of Defense Standard for Configuration Management*, 1997.

Handbook for Information Technology Security Certification and Accreditation Procedures, February 2003.

Handbook for Information Technology Security General Support Systems and Major Applications Inventory Procedures, March 2005.

Handbook for Information Assurance Security Policy, June 2005.

IEEE/EIA 12207, *Industry Implementation of International Standard ISO/IEC: ISO/IEC12207 Standard for Information Technology Software life cycle processes*, 1996.

ISO 10007, *Quality Management Guidance for Configuration Management*, 2002.

ISO/IEC 12207, *International Standards Organization: Implementation of Information Technology—Software Life Cycle Processes*, 1998.

MIL-HDBK-61A (SE), *Military Handbook for Configuration Management Guidance*, 2001.

National Institute of Standards and Technology (NIST), *Special Publication 800-12, Introduction to Computer Security: The NIST Handbook*, October 1995.

National Institute of Standards and Technology (NIST), *Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

Office of Management and Budget (OMB) Circular A-130, *Appendix III, Security of Federal Automated Information Resources*, November 2000.

Appendix D. Sample Change Request Form

Change Request Form

CR Originator (System Owner) Name:	**Priority:** ☐ **Critical** ☐ **Routine** ☐ **Administrative**	**CR Tracking Number**
CR Originator (System Owner) Signature: _____ **Date:**	**Title of Change:**	

Description of Change: ☐ **Continues on attached page**

Product Identification Impact, Software	☐ **Continues on attached page**
Product Identification Impact, Hardware	☐ **Continues on attached page**
Product Identification Impact, Documentation	☐ **Continues on attached page**

Security Impact:

Business Impact: ☐ **Continues on attached page**

Justification of Change and Potential Impact if Change is Not Made: ☐ **Continues on attached page**

Estimated Number of Staff/Total Hours Needed: **Staff** **Total Hours**	**Sites Affected:**

CR Sponsor's (SSO) Name:	**Signature:**	**Date:**

CCRB Name (to be completed by the CCRB): **Signature:**	**CCRB Disposition: If not "Approve," provide explanation.** ☐ **Approve** ☐ **Disapprove** ☐ **Defer** ☐ **Refer To** _____	**Date:**

Resolution

1. Testing	2. Implementation	3. Quality Assurance
Tester:	**System Owner Signature:**	**QA Signature:**
System Test Completion Date:	**Implementation Date:**	**QA Completion Date:**
Acceptance Test Completion Date:	**Additional Comments:**	**Documents Completed:** _____ _____
Additional Comments:		

Appendix E. Sample Security Impact Assessment Form

Security Impact Assessment Form

CR Originator (System Owner) Name:	**Priority:**	**CR Tracking Number**
CR Originator (System Owner) Signature:	☐ **Critical** ☐ **Routine** ☐ **Administrative**	
Date:	**Title of Change:**	

Description of Change (from CR Form):

Impact of the Change on System Security:

_____

_____

_____

_____

_____

_____

_____

_____

Sites Affected:

Will any security measures need to be suspended during the actual implementation time?

☐ **Yes** ☐ **No** **If yes, please explain below:**

_____

_____

_____

_____

_____

SSO Name:	**Signature:**	**Date:**

Appendix F. Sample Emergency Change Request Form

Emergency Change Request Form

Emergency Request No.: _____ Date of Request: _____

Name of System: _____ PO: _____

Type of Change (Hardware, Software, etc.): _____

Components Affected: _____

Users Affected: _____

Explain Security Impact (attach supporting documentation): _____

_____
_____
_____
_____
_____
_____
_____
_____
_____

Staff Hours and Labor: _____

Cost: _____

Date (Needed Implementation Date): _____

Justification (attach supporting documentation): _____

_____
_____
_____
_____
_____

_____ _____

SSO Authorized Signature **Date**

_____ _____

CCRB Authorized Signature **Date**

Appendix G. Sample Change Request Status Log

Change Request Status Log						
CR Number	**Assigned CCRB Reviewer Name**	**CR Disposition (Approve, Refer, Disapprove, Defer)**	**Date**	**Change Completion Projected Date**	**Actual Completion Date**	**Completion Sign Off**