Test\_2015-01-15-1052

[project ID not provided]

Configuration Management

Plan

Prepared for

Department of Homeland Security Headquarters (DHS HQ)

[Component address not provided]

[project version not provided]

16 January 2015

APPROVAL SIGNATURE

The Test\_2015-01-15-1052 Configuration Management Plan was prepared for the exclusive use of the Department of Homeland Security Headquarters (DHS HQ).

Approved by & Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Information System Owner

**DOCUMENT CHANGE HISTORY**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1.0 INTRODUCTION 1](#_Toc256000000)

[1.1 System Identification and Description 1](#_Toc256000001)

[1.2 Purpose 1](#_Toc256000002)

[1.3 Scope 1](#_Toc256000003)

[1.4 Structure 2](#_Toc256000004)

[2.0 ROLES AND RESPONSIBILITIES 2](#_Toc256000005)

[3.0 COMMUNICATIONS 3](#_Toc256000006)

[4.0 CONFIGURATION CONTROL PROCESS 3](#_Toc256000007)

[4.1 Step 1: Establish System Configuration Baseline 4](#_Toc256000008)

[4.1.1 System Architecture 5](#_Toc256000009)

[4.1.2 System Characterization 5](#_Toc256000010)

[4.1.3 Hardware 5](#_Toc256000011)

[4.1.4 Software 5](#_Toc256000012)

[4.1.5 System Library 6](#_Toc256000013)

[4.2 Step 2: Identify Change and Complete Change Request Form 6](#_Toc256000014)

[4.3 Step 3: Submit Change Request Form 7](#_Toc256000015)

[4.4 Step 4: Evaluate Change Request Form 8](#_Toc256000016)

[4.5 Step 5: Review Impact Analysis 8](#_Toc256000017)

[4.6 Step 6: Approve, Disapprove, Defer, or Refer Change Request 8](#_Toc256000018)

[4.7 Step 7: Perform Configuration Status Accounting 9](#_Toc256000019)

[4.8 Step 8: Conduct Configuration Verification and Audit 9](#_Toc256000020)

[5.0 CONFIGURATION MANAGEMENT RESOURCES 10](#_Toc256000021)

[5.1 Facilities 10](#_Toc256000022)

[5.2 Tools 10](#_Toc256000023)

[6.0 REFERENCE DOCUMENTS 11](#_Toc256000024)

# INTRODUCTION

## 1.1 System Identification and Description

System Number: [project ID not provided]

System Name: Test\_2015-01-15-1052

System Abbreviation:

The system is in the following system operational status: Not Specified

Deployment of Test\_2015-01-15-1052 began in [YEAR] with a core set of applications. Today, it is one of the most comprehensive integrated administrative information systems in the United States. Since workload reporting was an initial motivation for corporate databases, most of the Department of Homeland Security Headquarters (DHS HQ)'s corporate systems collect their information from Test\_2015-01-15-1052. Recent enhancements have clearly shifted the focus from workload to enabling the integration of administrative information from various disciplines, forming the basis for an automated and distributed information system.

## 1.2 Purpose

An information system is typically in a constant state of migration, with upgrades to hardware, software, or firmware and possible modifications to the system environment. Documenting information system changes and assessing the potential impact on the security of the system on an ongoing basis is an essential aspect of maintaining the security accreditation. A good Configuration Management Plan ensures that configuration and control changes to the system are monitored, evaluated, and impacts are assessed prior to implementation.

## 1.3 Scope

This Configuration Management Plan applies to the Test\_2015-01-15-1052managed by the Department of Homeland Security Headquarters (DHS HQ). It applies to all levels of the organization and all users of the system.

As a management tool, the CMP ensures that system components, whether hardware or software, are properly identified and controlled during the day-to-day operations at the Department of Homeland Security Headquarters (DHS HQ), provides a disciplined set of techniques for controlling changes to identified baseline security configurations, and enhances consistency, compatibility, integrity, and security of Department of Homeland Security Headquarters (DHS HQ) systems.

## 1.4 Structure

This plan is organized into five major sections:

* Section 1 provides an introduction to the plan.
* Section 2 provides a description of the CMP roles and responsibilities.
* Section 3 describes the communication methods related to this CMP.
* Section 4 provides an overview of the configuration control process.
* Section 5 discusses CM resources.
* Section 6 provides a referenced forms list.

# 2.0 ROLES AND RESPONSIBILITIES

This section clearly identifies CM roles and responsibilities for the system, noting that all CM activities must be performed in accordance with the processes and procedures documented in the CMP. Some examples of CM roles and responsibilities in an organization are provided in the following table.

| Role | Responsibilities |
| --- | --- |
| Chief Information Officer | Setting forth policies regarding CM and implementing CM at the highest level for the Department of Homeland Security Headquarters (DHS HQ). |
| System Owner/Manager | (Or other designated individual) serves as the authority for all matters of CM for the system. Responsible for developing functional requirements and verifying that the requirements are implemented appropriately. 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 | Oversees all aspects of the CMP; responsible for all day-to-day activities necessary to support the CMP, and may call on other personnel for assistance. Primary responsibilities are:  - 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 (CCRB) | Governing body for CM policy and guidance affecting all GSs and MAs in the organization. A chairperson should be appointed by the CCRB to oversee the activities of the Board. Primary 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 | Responsible for reporting any weaknesses identified in current versions of the hardware, software, and components. |
| Other | Other roles in the organization, such as the information system security officer (ISSO) and system administrator may also have specific CM responsibilities. Once the extent of these responsibilities is determined, they are documented in the CMP for the system. |

Table 2-1: Configuration Management Roles and Responsibilities

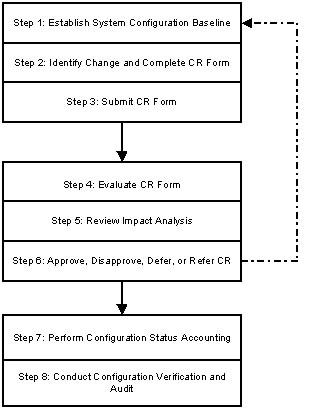
# 3.0 COMMUNICATIONS

{The communications section discusses the methods used to share information regarding CM (such as upgrades, application changes, technical notices, version control, and so on) within the organization. This section addresses items such as who has access to the information and how, when, and what type of information is shared.}

# 4.0 CONFIGURATION CONTROL PROCESS

This section identifies the processes/steps required to ensure that all changes to Test\_2015-01-15-1052are properly requested, evaluated, and authorized. Processes provide detailed, step-by-step procedures for establishing, processing, tracking, and documenting changes.

The Configuration Control Process is critical to the Test\_2015-01-15-1052because of the number of changes, revisions, upgrades, and modifications that it is expected to 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 the system. The figure below is an illustration of the Configuration Control Process currently in place.



The following sections provide detailed descriptions of the eight minimum steps that are included as part of the Configuration Control Process.

## 4.1 Step 1: Establish System Configuration Baseline

The first step of the Configuration Control Process is to establish the System Configuration Baseline as a snapshot of the current design and functionality of the system, 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 system is not yet operational, the System Configuration Baseline reflects the current status of the system within the System Development Cycle (SDC). Specifically, the following items describe and/or identify the System Configuration Baseline:

* System Architecture
* System Characterization
* Hardware
* Software
* System Library

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

### 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 Division or Organization, or external to other organizations.}

### 4.1.2 System Characterization

Purpose and functionality of the system:

* Number of users: *{Number of users}*
* System criticality and information sensitivity levels: *{System criticality and information sensitivity levels}*
* System confidentiality, integrity, and availability levels: *{System CIA levels}*
* Type of data that is processed by or stored in the system: *{Type of data processed or stored}*

### 4.1.3 Hardware

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Manufacturer's Name | Model Number | Serial Number | Configuration Settings | Hardware specifications, parts, and/or boards |
|  |  |  |  |  |

### 4.1.4 Software

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Title (including acronym or nickname) | Version Number | Build Number, if appropriate | Media (such as 4mm tape, 8mm tape, CD ROM, and so on) | Hardware requirements necessary to run the software (such as available disk space, random access memory (RAM), network connections, and so on) | Control parameters (such as 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, and so on) |
|  |  |  |  |  |  |

### 4.1.5 System Library

#### 4.1.5.1 System Documentation and Supporting Information

The following system documentation was used to establish the System Configuration Baseline:

|  |  |  |  |
| --- | --- | --- | --- |
| Title | Publication Date | Version Number | Revision Date |
|  |  |  |  |

#### 4.1.5.2 CM Library

The CM library contains all CM-related documentation (such as change request (CR) forms, security impact assessment forms, and CR status logs, and so on). The CM Manager is responsible for maintaining the CM library to ensure that all documents regarding system changes are stored in an orderly manner, and copies are provided to authorized persons, when necessary. Due to the complex nature of the Test\_2015-01-15-1052and frequency of updates and changes, the CM manager has delegated 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 Change Request Form

To initiate a change, the need for that change is 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}* is collected. Changes to the Test\_2015-01-15-1052are categorized as:

**Emergency** - any change that is required to address safety or security issues

**Major** - any change that requires more than 120 hours of development support

**Minor** - any change that requires less than 120 hours of development support

**Optional** - any change that is strictly "nice to have" but is not necessary to the function of the system

The CR form provides information such as title and description of the change, justification, timeframe, and the potential impact on security, including a signature from the approving security official.

The system owner or other designated individual ensures that all information on the form has been completed before submission.

A security impact assessment form is included with the CR form, describing in detail the possible impact that this change could have on system security.

See Section 6, Figures 1 and 2, for a sample change request form and sample security impact assessment form.

## 4.3 Step 3: Submit Change Request Form

The completed CR form is submitted to the CCRB for approval. Upon receipt, a tracking number is assigned to and documented on the CR form. All emergency CR forms are submitted to the CCRB for approval in a less critical timeframe and an emergency request number is assigned to and documented on the emergency CR form. In addition, the CCRB updates the CR status log to include all new CRs, including emergency requests, so the change can be tracked.

Not all system configuration changes need to be approved by the CCRB. For example, changes to a 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 are tracked in either a CR status log or in an equivalent log that maintains all configuration changes.

See Section 6, Figure 3, for a sample change request status log.

## 4.4 Step 4: Evaluate Change Request Form

In Step 4, the CCRB carefully evaluates 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 provides details on how the evaluation is performed and establishes 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 reviews the technical and business effects of implementing the change to the system. The technical analysis, usually conducted first, determines 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
* All security components affected

The business analysis should determine the following:

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

The CCRB must consider the results of the impact analysis review before making a decision about the change.

See Section 6, Figure 2, for a sample Security Impact Assessment Form.

## 4.6 Step 6: Approve, Disapprove, Defer, or Refer Change Request

The CCRB reviews the CR and Impact Analysis and makes a decision based on the information provided. The CR status log is used to track all CRs 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.

## 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 of all systems in the CM process
* Tracks changes and action items

## 4.8 Step 8: Conduct Configuration Verification and Audit

The final step of the Configuration Control Process 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 that physical configuration audits ensure that 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 is 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 (test results, vendor documentation, system environment, and configuration identification information, etc.)
* The system performs its functions
* Security status is constant

# 5.0 CONFIGURATION MANAGEMENT RESOURCES

{The CM resources section of the CMP describes facilities and tools used for CM activities. This information serves as guidance for planning the resources required to support the functions of each organization throughout the CM process. Because the number of staff, equipment, and space required varies according to each organization's needs, the CM manager periodically reviews the resources involved in CM and verifies that the facilities and tools are up-to-date. The CM manager also works with the system owner and CCRB to determine what type of software package is best for the Organization and its systems.}

## 5.1 Facilities

{Facilities consist of dedicated spaces for personnel and equipment. Security controls must be in place to safeguard the materials based on confidentiality and sensitivity requirements. This section includes physical and environmental security controls that must be in place to protect the system.}

## 5.2 Tools

{Using automated tools is an effective way of managing CM activities and maintaining change control. This section identifies any commercial off-the-shelf (COTS) software packages, automated software, or support hardware and software that are used to build and manage the system.}

# 6.0 REFERENCE DOCUMENTS

CHANGE REQUEST FORM

|  |  |  |
| --- | --- | --- |
| CHANGE REQUEST FORM | | |
| **Requirement #** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **CRF #** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Originator: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_ Release # \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Originator email: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Originator Phone: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Type:  [ ] New Requirement [ ] System Problem [ ] Suggestion for Improvement  [ ] Requirement Change [ ] User Interface Problem [ ] Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  [ ] Design Change [ ] Documentation Correction  Priority:  [ ] Emergency [ ] Major [ ] Minor [ ] Optional  Description:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_    Please attach supporting documentation of the requested change (screen/report printouts, document pages affected, etc.). | | |
| Status | Date | Signature/Comments |
| Reviewed & Estimated |  |  |
| On Hold |  |  |
| Canceled |  |  |
| Approved for Change |  |  |
| Code Updated |  |  |
| Documentation Updated |  |  |
| Completed |  |  |
| CFR #\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **New Release #** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Please attach supporting documentation for review & estimates (analysis, resource estimates, layouts, document pages affected, etc.) | | |

Figure 1. Sample Change Request Form Template

SECURITY IMPACT ASSESSMENT FORM

|  |
| --- |
| SECURITY IMPACT ASSESSMENT FORM |
| Priority:  [ ] High [ ] Medium [ ] Low  CR Originator  (System Owner)  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title of Change: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ CR Tracking Number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  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. |

Figure 2. Sample Security Impact Assessment Form Template

CHANGE REQUEST LOG

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CHANGE REQUEST LOG | | | | | | | | | | | |
|  | | | | Approval | | Status | | | | | |
| Request # | Reqmnt # | Date Submitted | Priority (E, MA, MI, OPT)\* | Change Approved | Change Not Approved | Hold (Future Enhancement) | Technical Evaluation Phase | Change In Progress | Canceled | Target Date | Date Complete |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |

\* E = Emergency, MA = Major, MI = Minor, OPT = Optional (as defined by the Change Request Form)

Figure 3. Sample Change Request Log Template